



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**TRUST AND INFLUENCE IN THE INFORMATION AGE:
OPERATIONAL REQUIREMENTS FOR
NETWORK CENTRIC WARFARE**

by

Nicole Ilene Blatt

December 2004

**Thesis Advisor:
Thesis Co-Advisor:**

**Dorothy Denning
Scott Jasper**

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2004	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Trust and Influence in the Information Age: Operational Requirements for Network Centric Warfare			5. FUNDING NUMBERS	
6. AUTHOR(S) Nicole I. Blatt				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) <p>Military leaders and scholars alike debate the existence of a revolution in military affairs (RMA) based on information technology. This thesis will show that the Information RMA not only exists, but will also reshape how we plan, operate, educate, organize, train, and equip forces for the 21st century.</p> <p>This thesis introduces the Communication Technology (CommTech) Model to explain how communication technologies affect organizations, leadership styles, and decision-making processes. Due to the growth in networking enterprises, leaders will have to relinquish their tight, centralized control over subordinates. Instead, they will have to perfect their use of softer power skills such as influence and trust as they embrace decentralized decision-making.</p> <p>Network Centric Warfare, Self-Synchronization, and Network Enabled Operations are concepts that provide the framework for integrating information technology into the battlespace. The debate that drives centralized versus decentralized control in network operations is analyzed with respect to the CommTech Model. A new term called Operational Trust is introduced and developed, identifying ways to make it easier to build trust among network entities. Finally, the thesis focuses on what leaders need to do to shape network culture for effective operations.</p>				
14. SUBJECT TERMS			15. NUMBER OF PAGES	
Information RMA Network Centric Warfare Communications Technology Model			113	
Trust Network Enabled Operations Centralized Control			16. PRICE CODE	
Influence Self-synchronization Decision-Making				
Leadership Operational Trust Decentralized Execution				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**TRUST AND INFLUENCE IN THE INFORMATION AGE:
OPERATIONAL REQUIREMENTS FOR NETWORK CENTRIC WARFARE**

Nicole I. Blatt
Major, United States Air Force
M.S., University of Southern California, Aerospace Engineering, 1993
B.S., United States Air Force Academy, Astronautical Engineering, 1990

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(DEFENSE DECISION-MAKING AND PLANNING)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2004**

Author: Nicole I. Blatt

\

Approved by: Dorothy Denning
Thesis Advisor

Scott Jasper
Thesis Co-Advisor

James Wirtz
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Military leaders and scholars alike debate the existence of a revolution in military affairs (RMA) based on information technology. This thesis shows that the Information RMA not only exists, but also will reshape how the U.S. Military plans, operates, educates, organizes, trains, and equips forces for the 21st century. Every aspect of the DOTMLPF¹ process will be affected by the exponential growth in accessibility to information.

This thesis introduces the Communication Technology (CommTech) Model to explain how communication technologies affect organizations, leadership styles, and decision-making processes. Due to the growth in networking enterprises, leaders will have to relinquish their tight, centralized control over subordinates. Instead, they will have to perfect their use of softer power skills such as influence and trust as they embrace decentralized decision-making.

Network Centric Warfare, Self-Synchronization, and Network Enabled Operations are concepts that provide the framework for integrating information technology into the battlespace. The debate that drives centralized versus decentralized control in network operations is analyzed with respect to the CommTech Model. A new term called Operational Trust is introduced and developed while identifying ways to make it easier to build trust among network entities. Finally, the thesis focuses on what leaders need to do to shape network culture for effective operations.

By understanding the information technology changes and how they affect all aspects of operations, we will be better prepared for the future global environment. The military must be prepared to transform its force structure, doctrine, strategy, and tactics to co-evolve with technology. All warfighters should consider how to best exploit information to increase our combat capability.

¹ DOTMLPF stands for doctrine, organization, training, materiel, leadership, personnel, and facilities. It is the Department of Defense's method to ensure all aspects of a plan or concept are thoroughly scrutinized.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

INTRODUCTION.....	1
A. The Information RMA – It’s Real And It’s Here!	1
B. How This Thesis Is Organized	3
CHAPTER 1. THE COMMUNICATIONS TECHNOLOGY MODEL	5
A. The Computer Technology Timeline.....	5
B. Why This Is Important – The CommTech Model.....	7
C. How to Prepare For the 21st Century Networked Organization.....	10
D. What To Expect.....	11
E. Summary	12
CHAPTER 2. PROVING THE COMMTECH MODEL.....	13
A. Introduction	13
B. The 1970s.....	14
1. Industry in The 1970s	14
2. The 1970s Military	15
3. Nuclear Inter-Continental Ballistic Missiles	15
4. Vietnam and the Raid on Son Tay.....	16
C. The 1980s.....	17
1. Industry in The 1980s	17
2. The 1980s Military	18
3. The Libya Bombing	20
4. Desert One, The Iran Hostage Rescue Fiasco	21
D. The 1990s.....	22
1. Industry in The 1990s	22
2. The 1990s Military	23
3. Desert Storm.....	25
4. Somalia.....	25
E. The 2000s.....	27
1. Industry in The 2000s	27
2. The 2000s Military	28
3. Operations Enduring and Iraqi Freedom	28
4. OIF2 Abu Ghraib Prison.....	29
F. Is The Military Stuck in the 1990s?	30
1. Reduction of Military Research and Development.....	31
2. Military Downsizing.....	31
3. Counterintuitive to Military Mindset.....	32
G. Evidence We Are On Our Way.....	32
H. Summary	33
CHAPTER 3. UNDERSTANDING NETWORK CENTRIC WARFARE, SELF- SYNCHRONIZATION, AND NETWORK ENABLED OPERATIONS.....	35
A. Introduction	35
B. The Debate	36

C. The Basics of NCW	38
D. Key Concepts	40
E. Methods of Information Sharing	43
F. Transitioning to Self-Synchronization	45
G. Envisioning Network Enabled Operations	47
H. Issues with Networks.....	49
I. Can Self-Synchronization Be Achieved?	52
J. Summary	53
CHAPTER 4. BUILDING OPERATIONAL TRUST.....	55
A. Introduction	55
B. A Definition of Trust	56
C. Moving from Blind to Reasoned Trust.....	58
D. Operational Trust.....	59
E. How Operational Trust Factors In – Why It is Important to Network Centric Warfare	61
F. Understanding the Need to Trust	62
Step 1. Determining the Need to Trust: <i>Do I have to make a bet?</i>	63
Step 2. Assessing the Risk: <i>What are the stakes of the bet?</i>	64
G. Finding Ways To Make It Easier To Trust.....	67
Step 3. Changing the Odds: <i>Can I make a safer bet?</i>	68
H. A Real-World Example of Trust in the Decision Process.....	74
I. Summary	75
CHAPTER 5. NETWORK LEADERSHIP STRATEGY AND TACTICS	77
A. Introduction	77
B. Leadership Strategy	77
C. Influence Techniques – Specific Tools for Soft Power	81
1. Provide a Reason.....	81
2. Gain Commitment	82
3. Start Early	83
4. Benefit from Reciprocity	84
5. Appearance Builds Respect.....	84
6. Build a Cohesive Team	85
7. Choose the Technique to Fit in Context.....	86
D. Some Final Thoughts For Implementation	86
1. Create Capability Thread Teams	86
2. Create Competition Exercises.....	87
3. Create Reputation Scores.....	87
4. Cultivate a Dedicated Infrastructure Force	88
5. Simplify the Process for Innovation	88
6. Visit the Squadron Bar	89
E. Summary	90
CONCLUSION	91
BIBLIOGRAPHY	93

INITIAL DISTRIBUTION LIST97

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1-1. The Computer Technology Timeline.....	5
Figure 1-2. CommTech Model Applied to Leadership and Decision-Making	8
Figure 2-1. The CommTech Model Applied to Commercial Industry and Military Organizations & Operations.....	13
Figure 3-1. The Network Centric Warfare Process.....	39
Figure 3-2. Comparison Between 1 st and 2 nd Generation Network Operations.....	46
Figure 3-3. Expansionist View of Network Enabled Operations with Self- Synchronization Processes Embedded in the Overall Operations	48
Figure 4-1. Moving from Blind Trust to Reasoned Trust	59
Figure 4-2. Risk Assessment Matrix for the Potential Consequences of Misplaced Trust	65

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I know I am truly privileged to have had this incredible opportunity to spend eighteen months in Monterey at the Naval Postgraduate School (NPS). I would like to express my appreciation, first, to the Air National Guard Air Force Reserve Test Center (AATC), who trusted me enough to send me on such excellent adventures from the test ranges in Nevada to the sands of Iraq. Their unwavering support got me to Monterey in the first place. I am grateful for the chance to learn from such great professors as Dr. Dorothy Denning, CAPT Scott Jasper, and Dr. John Arquilla. Thanks to Shane Deichman at JFCOM, who always immediately put everything aside to help me, whether it was to find a contact or offer TDY funds for research. Dr. David Alberts and his team in the DoD Command and Control Research Program (CCRP) invited me to present my work on Trust at the International Symposium in Copenhagen, Denmark. Thanks for a great trip, and I love the iPod! I am indebted to the Joint Expeditionary Force Experiment (JEFX) staff, especially LtCol Brian Searcy, who gave me full access to all people and processes in the Combined Air Operations Center (CAOC). Thanks to Jeffrey Kegler and all my Mermaid neighbors for their willingness to discuss Trust and Influence over wine on Thursday nights. Moreover, I would not have made it this far without the much needed support and encouragement from my Mom. Thanks Mom! And finally, I want to express a special thank-you to my mentor, colleague, and friend, Colonel Lou “Schwack” Durkac, whose numerous phone conversations helped me flesh out (or isn’t it “flush out”?) the ideas in this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

A. The Information RMA – It's Real And It's Here!

The information revolution is real and it is happening now! Advances in information technology create new capabilities, and those capabilities affect how we work, live, and even fight wars. Military leaders and scholars alike debate the existence of a revolution in military affairs (RMA) based on information technology. This thesis shows that the Information RMA not only exists, but also will reshape how the U.S. Military plans, operates, educates, organizes, trains, and equips forces for the 21st century. Every aspect of the DOTMLPF² process will be affected by the exponential growth in accessibility to information.

This thesis introduces the Communication Technology (a.k.a. CommTech) Model to explain how communication technologies affect our organization, leadership style, and decision-making process. Due to the growth in networking enterprises, leaders will have to relinquish their tight, centralized control over subordinates. Instead, they will have to perfect their use of softer power skills such as influence and trust as they embrace decentralized decision-making.

Network Centric Warfare and Network Enabled Operations are concepts that provide the framework for integrating information technology into the battlespace. Some see this technology as a way to micromanage and direct tactical operations, greatly increasing a commander's ability to centrally control operations. Others see the network as a way to provide shared knowledge, thus allowing decentralized control and shared authority across the battlespace. While this debate regarding how best to operate in a networked environment continues, both camps clearly see the benefits of shared situational awareness. Consequently, it is crucial that Dept of Defense get the technology, and hence capability, to the warfighter in the field.

² DOTMLPF stands for doctrine, organization, training, materiel, leadership, personnel, and facilities. It is the Department of Defense's method to ensure all aspects of a plan or concept are thoroughly scrutinized.

For networked operations to succeed, operational trust becomes ultra-important. It is easy to say everyone should trust each other, but that is not realistic. Many people, especially military people, will not blindly trust other entities, be it people, objects, systems, or technology. They need a reason to trust and a method to assess it. However, the interdependency that accompanies network centric warfare requires a level of operational trust to accomplish the mission. Therefore, it is necessary to find ways to make it easier to build trust among network entities.

Networking enables every individual from the top battle commander to the lowest echelon fighter to share information and gain increased situational awareness. By pushing the “power to the edge” – allowing the actors on the edge of the command and control structure to make their own *informed* decisions and act in accordance with the command intent – leaders can exponentially multiply the number of simultaneous events occurring within an operation, thus magnifying the efficiency and effectiveness of the mission. Incredible new capabilities will develop out of grass-roots squadrons, companies, or teams, and they will propagate their ideas across a web of multiple, redundant communication paths. But this shared knowledge can be a double-edged sword.

Since sharing information allows individuals to be more knowledgeable, they now are capable of making their own decisions with increased confidence. Moreover, with access to the internet, any individual or team can make their voice heard. Therefore, rank within a hierarchical organization becomes less relevant as a source of power. Without direct control of information flow, commanders can no longer expect to maintain strictly hierarchical corridors of power, as their subordinates question orders or find ways around roadblocks in the chain of command.

Therefore, leaders must create the vector. Innovative capabilities will rise from the bottom-up, providing the magnitude. Leaders must provide the vision – the direction – to drive the organization forward. Commanders must communicate a clear, consistent message that includes (but is not limited to) command intent, guidance, objectives, operational priorities, rules of engagement, and ethics. With decentralized decision-making, lower-level troops need to understand the significance of their orders. They

need to know the answer to the question, “Why is my task important?” Leaders must learn the skills to influence their subordinates, peers, and even their commanders, if they want to hold power in the Information Age. Rosalynn Carter said it well. "A leader takes people where they want to go. A great leader takes people where they don't necessarily want to go, but ought to be."³

B. How This Thesis Is Organized

This thesis is organized into five chapters. Chapter 1 introduces the CommTech Model and explains its significance for the 21st century. It suggests ways to prepare for the age of network enterprises and what to expect in the near future. Chapter 2 is dedicated to proving that the CommTech Model is valid. By comparing the model to both commercial and military historical events over the last four decades (since computers became commonplace), we can see the trends that align with the model. From there, we can predict how organizations, leadership style, and decision-making processes will change as networking power is distributed in the 21st century. Chapter 3 specifically addresses the military applications of communications technology by explaining the concepts of network centric warfare, network enabled operations, and self-synchronization. In this chapter the debate that drives centralized versus decentralized control in network operations is analyzed. Because trust is such an important part of efficient network operations, Chapter 4 is dedicated to understanding trust and finding reasons to trust. A new term called *Operational Trust* is introduced and developed. This chapter also suggests ways of improving an individual’s trust-based decisions. Finally, Chapter 5 focuses on what leaders need to do to shape network culture for effective operations. This chapter discusses the shift towards softer power to influence and guide subordinates, peers, and superiors. It also includes specific ideas to “operationalize” trust in networks.

Communications Technology has changed the way we organize and operate in business, in war, and in life. By understanding what the changes are and how they affect

³ Brainyquote.com. http://www.brainyquote.com/quotes/authors/r/rosalynn_carter.html. 1 December 2004.

all aspects of operations, we will be better prepared for the future global environment. The military must be prepared to transform its force structure, doctrine, strategy, and tactics to co-evolve with technology. All warfighters should consider how to best exploit information to increase combat capability.

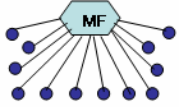

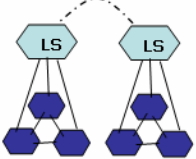
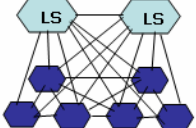
CHAPTER 1. THE COMMUNICATIONS TECHNOLOGY MODEL

A. *The Computer Technology Timeline*

Over the last four decades, the computer has changed the way we live. From limitless programming capabilities to business applications and now as part of everyday life, the computer has reshaped our daily activities. However, the implications of the information revolution go far beyond the direct usage of these electronic boxes. New capabilities have reshaped government organizations, commercial industry management, military force structure, and strategic decision-making. And these changes, amazingly, follow the same patterns as the computer network architecture advancements themselves.

If you think of computer programs as the equivalent of decision makers in a communications technology domain, then you see that organizations and decision-

The Communications Technology Timeline

Timeline	1970s	1980s	1990s	2000s
Computer Technology	Mainframe + Terminals 	Personal Computers (PCs) 	Local Area Network of PCs 	Internet and Intranets, DSL, Access to the Web 
Characteristics	Few actual "thinkers" Queued processes Long timelines	Isolated decision-making, No connectivity	Integration & synergy within local networks Weak external connections	Peer-to-peer relationships Easy access Exponential capability

MF = Mainframe LAN = Local Area Network
LS = LAN server DSL = Digital Subscriber Line

Note: Computer Programs = Decision-Makers in the Communications Technology Domain

Figure 1-1. The Computer Technology Timeline

making styles have followed the same pattern as the computer architecture throughout the decades. Figure 1-1 explains the changes in computer technology over time.

In the 1970s, computer network architecture was designed to have a mainframe computer with several terminals. Without embedded computer programs, these terminals were slaves to the mainframe and could only be used as input/output devices. All decisions were centralized at the mainframe computer. Computer programs took hours to compile and run as they waited in the queue for processing time. On some mainframe systems, it was required that a programmer reserve computer-processing time to complete his projects.

With the 1980s came a giant leap in computer technology, and the personal computer (PC) was born. Personal computers held their own programs and could therefore make their own decisions. People were no longer required to wait for processing time of the single centralized mainframe. Instead, individuals were free to process their own work projects. Personal computers, however, were generally not interlinked. This lack of connectivity resulted in isolated computer processing and decision-making.

By the beginning of the 1990s, local area networks formed. Within an organization, computers became networked together. The e-mail became a medium for communication as individuals within an organization began sharing data and internal organizational decisions. This sharing within an organization created synergy by combining the strengths of individuals or small groups within the organization for greater effects. The individuals that actually typed at the keyboard became the users, not just the computer programmers. While connectivity within the organization strengthened, however, sharing that data with other organizations proved to be difficult. Furthermore, when the messages did make it to another organization, they were often misunderstood or dismissed.

At the dawn of the 21st century, a network architecture has emerged that supports both the internet and intranets. As individuals and organizations begin to populate the networks with information, the information superhighway takes shape. Accessibility to

the web has greatly improved. People are no longer dependent on single expensive servers at organizational headquarters to gain access to information. By subscribing to one or more internet service providers (ISP), users now have multiple access points to enter the web whether at work, at home, or even at Starbucks. Besides having multiple access points, the speed at which we can retrieve or broadcast information has greatly increased. Twenty-eight kilobyte modems have been replaced with high speed DSL and cable modems for quicker access at home. WiFi provides high speed data connectivity throughout airports, universities, and shopping malls. Now, not only do individuals have multiple ways of receiving and sending data, they can do so at greater than 1,000 times the speed of previous systems. This equates to an exponential gain in accessibility to information.

B. Why This Is Important – The CommTech Model

Why does it matter what communications architecture is in place? Because new technological capabilities drive different leadership styles and decision-making strategies. And these differences affect the way we shape organizations, conduct business, run operations, and fight wars. A constant struggle persists in leadership styles between hard-line control on one side versus softer influence and trust on the other. As technology provides new capabilities, leadership styles and attitudes must adjust to fit the new capabilities. Decision-making varies between centralized and decentralized as the source of power from information accessibility changes. This is illustrated in Figure 1-2, The CommTech Model (short for “Communications Technology”).

In the 1970s, the mainframe architecture and centralized organizational style created leaders with an inordinate amount of power over their subordinates. It also led to centralized control and decision-making. A consequence of this centralized power, however, was the slow process by which decisions were made. Delegation of authority was minimal with only a few authorized to make key decisions. The bottleneck created for approving plans or ideas degraded the speed of command. In the military, the focus was on procedural training and practice to increase the speed of execution once the orders were given.

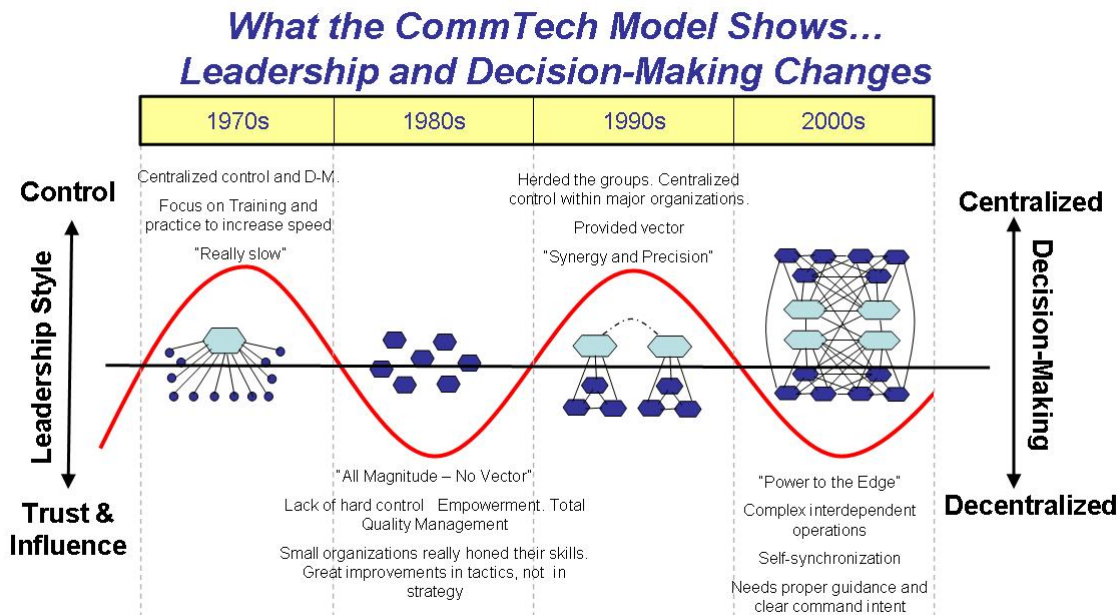


Figure 1-2. CommTech Model Applied to Leadership and Decision-Making

With the PC boom of the 1980s, leaders lost that centralized control and had to create new ways to exert their power. Through this decade, leaders used influence to guide their subordinates. Without direct control, they were required to trust that the sub-organizations would do a good job. Company consultants taught corporate heads to focus on empowerment and total quality management. Small groups created great new capabilities and really honed their skills.

Unfortunately, although individuals and small teams were capable of making decisions on their own in the 1980s, they were not capable of working together in large organizations. This was a period of “all magnitude – no vector.” Incredible improvements were made in tactics, but not necessarily in strategy. Knowledge, ideas, and decisions were not shared outside the lowest levels of the organization. Nonetheless, as long as it was possible to assign specific objectives to individuals or small groups, and the operations could be deconflicted, these tasks could be accomplished with excellent results.

In the 1990s, a local area network (LAN) made it possible to herd together the individuals and small teams. Centralized control within major organizations came back into favor. This provided the direction – the vector. The capability increase of the lower or edge organizations combined with the direction from above created synergy.

In the 1990s, the original concept of Network Centric Warfare was born. Linking information from multiple sources reduced errors in decision-making, leading to better precision with increased confidence. Information was channeled vertically allowing top-level commanders to make decisions and centrally control operations. Once again, leaders did not need to put as much trust into their subordinates to make proper decisions because they could monitor all activities. With the new network technology creating the ability to control and monitor subordinate actions, commanders were able to synchronize tactical events for precise strategic effects.

Finally, in the 21st century, the webbed network of multiple organizations creates “power to the edge.” What that means is organizations that are on the edge of the command and control network, the effectors, can now gain access to the specific information they need, make their own decisions, and act upon those decisions. The networks enable operations to take place in a decentralized manner. This process of edge teams conducting their own decentralized decision-making and action within the context of the command intent is called self-synchronization. (This will be discussed in detail in Chapter 3). Because multiple decisions can occur simultaneously, the tempo of operations can increase exponentially.

In this latest decade, peer-to-peer relationships across organizational lines occur with ease. In fact, organizational lines blur as people can quickly and efficiently communicate with anyone at any level, both internally and external to their own group. Moreover lower-level workers have access to spreading their own words, thoughts, and ideas. The commanders do not have the same level of control as in the past because of the difficulty in trying to control information flow or access. Since this is a major source of hard power, their power dwindles as subordinates gain access to information from multiple, redundant sources outside normal channels. Instead, commanders must rely on influencing others and building trust among entities.

C. How to Prepare For the 21st Century Networked Organization

As seen in the CommTech Model, control is out – influence is the key to successful leadership in the new networked organizations. Leaders need to communicate a clear, consistent message to subordinates to ensure they direct their efforts in a manner that aligns with the overall strategy. In addition, because individuals are knowledgeable, they will not blindly follow orders as easily as in the past. They demand an understanding at the lowest echelons so they can best decide the appropriate actions to carry out orders. Furthermore, they must believe in and pass on to others the same message that the leaders are espousing. Therefore, it is critical to have clear executive vision and command intent for any operation. Included in this must be the operational priorities, functional doctrine, operational perspectives, proper guidance, ethical standards, appropriate rules of engagement, and well-defined roles and accountabilities.

It takes trust for networked forces to function efficiently. As operations become more complex, no single entity can do the job alone. Interdependencies become more important. Linking information from multiple sources adds another degree of complexity to an already complex mission. The more entities that are involved with sharing information and dividing tasks, the more the requirement for trust grows. Operational Trust is the lynchpin in all networked operations.⁴

Due to the uncertainties of near-future threats, the United States needs to be prepared to fight any enemy, anywhere, at any level of conflict, from enforcing sanctions and capturing terrorists, to full-scale theater operations and nuclear war. The U.S. Military requires agile and adaptable command and control networks to respond to any given situation. This will require synergistic networks to provide the accuracy, relevance, and timeliness of information under an increased operations tempo. The organization to meet these needs requires a leadership style characterized by influence and trust.

⁴ Operational Trust will be discussed in detail in Chapter 4.

D. What To Expect

As members of organizations realize the potential of the new communications technology, several changes will occur. Many of these trends have already materialized. Here are a few examples of what to expect:

- Decision Makers will be Younger – As technology improves, routine tasks become automated. The airline industry's transition to computerized check-in kiosks is an example of simple service related jobs disappearing. With fewer jobs that require simple tasking, entry level workers will take on the tasks that computers have not mastered, specifically complex decision-making. If you are not a decision maker, you might as well be automated.
- Organizational Standing Becomes Less Relevant – As agile networks form and dissolve to support operations, so will ad hoc organizations, such as Joint Task Forces. Standing organizations, regardless of where they fit in a wire diagram, will be relevant only depending on what capabilities they bring to the table. If they add benefit, they will be used; if not, they will be overlooked. Examples of unconventional tasking are the Air National Guard and Coast Guard taking on important roles in foreign wars.
- Lower Ranking People Will Have More Power – This power comes directly from the network. To maintain control of subordinates, some commanders may be tempted to control the flow of information. However, information denial is unrealistic when redundant multi-path networks are formed, especially when the new soldier depends on the network to accomplish his mission. There will always be ways around roadblocks on the information superhighway. With access to information, lower ranks will be better informed than past generations were. This leads to better decisions and ideas from younger people. When they want their ideas heard, they can disseminate them in many more directions than just the chain of command. With the internet, everybody has access to a soapbox.
- Innovative Projects Will Surface in the Field Without Certification – With unlimited access to knowledge and information, ideas will rise from unexpected sources. Edge organizations will create new capabilities or transform existing systems for new purposes.

If they are unsuccessful convincing superiors of the benefits, they will advertise them to their peers outside organizational lines. The Battlefield Universal Gateway Equipment (BUG-E) is an example of this kind of project. This equipment tied together several data links enabling joint forces to share position data across the Iraqi western desert. However, while the BUG-E was assembled and fielded in time for the war, the Air Staff requirements approval process took several months longer.

E. Summary

The CommTech Model demonstrates how innovations in information technology have shaped the way we lead organizations and operations. There is a constant struggle in leadership styles between tight control and the softer trust and influence. Accompanying this leadership issue is the tug-of-war between centralized and decentralized decision-making. We have entered a period where the graph indicates we must be prepared to use influence and trust to lead operations and decentralized decision processes to maintain operational tempo. The next chapter will provide evidence to prove the CommTech model, while the follow-on chapters will discuss how to address the issues raised by the model.

CHAPTER 2. PROVING THE COMMTECH MODEL

A. Introduction

The Information RMA will reshape all aspects of the military. Technology creates new operational capabilities and those new capabilities drive new leadership styles, decision-making processes, and organizational structures.

The CommTech Model Applied


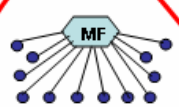

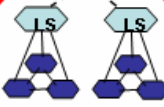
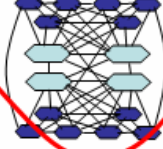
Timeline		1970s	1980s	1990s	2000s
Computer Technology Centralized Control  Decentralized Trust & Influence		Mainframe + terminals 	Personal Computers (PCs) 	Local Area Network of PCs 	Internet and Intranets, DSL, Access to the Web 
		Characteristics Few actual "thinkers" Queued processes Long timelines	Isolated decision-making, No connectivity	Integration & synergy within local networks Weak external connections	Peer-to-peer relationships Easy access Exponential capability
		Shape of Commercial Industry Organizations Large companies with giant factories & lots of workers: Ford, GM, IBM, Bethlehem Steel	Small business boom: Home offices, Apple Vision statements, Total Quality Mgt	Consolidators: Kraft, Target, Wal-Mart, Microsoft	Exponential growth on virtual communities and markets: eBay, Google
		Shape of Military Organizations and Leadership Styles Large brigades, Fewer generals and commanders (decision-makers) per capita, Lots of troops	Small teams, Task Forces, Push towards decentralization, Empowerment, Total Quality Mgt, Units can't work together well	Federated but connected at top central points, Those points only weakly connected outside of organization, strong service culture	Joint Task Forces, Shared information, Multiple redundant paths for information sharing, Decentralized DM at individual level
		Characteristics of Military Operations Centralized, synchronized, slow	Separate small team events, Deconfliction	Large deconflicted operations	Important information dimension, Shared SA Joint
Military Operation Examples	Good	Cold War Nuclear ICBMs Ops	Libya bombing (Op El Dorado Cyn)	Desert Storm	Operation Iraqi Freedom Western War
	Bad	Raid on Son Tay (Viet Nam)	Desert 1 (Iran), Grenada	Mogadishu, Somalia	OIF2, Abu Ghraib (Iraq prison)

Figure 2-1. The CommTech Model Applied to Commercial Industry and Military Organizations & Operations

The CommTech Model illustrates this point and predicts what we need to be ready for in the near-term future. However, is the model accurate?

This chapter is dedicated to proving the CommTech Model. Through a series of research theories, examples, and vignettes, this chapter explains how the model has been “operationalized” in commercial industry and military organizations throughout the decades. Figure 2-1 is a table of the CommTech Model applied to both commercial and military organizations and operations.

B. The 1970s

1. Industry in The 1970s

Gareth Morgan, a leading management researcher and prolific writer, states, “Computers are two-edged swords. They bring promise of liberation from toil and routine, yet often end up just intensifying systems of control.”⁵ The 1970s introduced computers to the workplace, and for the first time, workers worried about losing their mindless jobs to mindless machines. Management styles had remained relatively unchanged since the industrial revolution created the assembly line. The way business stayed competitive was for management to standardize processes to make workers work faster. Staff experts did the thinking for the laborers so that they could concentrate on working. The difference now was the new machines created even faster assembly lines with which the workers had to keep up. Efficiency meant imposing on workers the absolute power of management to control production. At General Motors, one assembly line operator complained in a 1974 interview, “I don’t even feel necessary....They could always find somebody stupider than me to do the job.” GM management did not trust the employees and frequently monitored the work. GM instituted a policy of mandatory overtime and refused to authorize sick leave without a doctor’s note. In some cases,

⁵ Morgan, Gareth, *Creative Organization Theory*. SAGE Publications, California, 1989. p. 59.

doctors were sent to workers' homes in an effort to curb absenteeism.⁶ The original computers in the workplace gave management the opportunity to gain even greater control over labor.

2. The 1970s Military

Military organizations during the Cold War had similar aspects. The fighting forces were large. The army unit of battle was a division of approximately 25,000 troops. American troops numbered in the several thousands under each O-6 (colonel) with decision-making responsibilities. Because of this organizational structure, decision-making was an extremely slow process involving waiting to get the commander's time so each decision could be made. The percentage of generals per capita was extremely low. Troops carried the workload. Training focused on following procedures and explicit orders. Efficiency improved by increasing the speed of execution. Although this style of leadership worked for the Cold War, it did not necessarily work for unconventional operations.

3. Nuclear Inter-Continental Ballistic Missiles

With the Cold War as our priority, the 1970s-style centrally controlled organization was an expected practice for the military when considering the possibility of launching nuclear intercontinental ballistic missiles (ICBMs). Centralized command and control helped maintain the proper balance of risk between nuclear security and nuclear surety.⁷ For instance, launching a nuclear weapon requires authorization from the president – he controls the launch codes. But it takes more than just the president's authorization to launch. After receiving authorization and authenticating the message source, the launch requires at least four people in two different locations to execute the launch order simultaneously. Missile combat crews train and compete in annual events to

⁶ Morgan, Gareth, *Creative Organization Theory*, p.55. This selection comes from "Lordstown: Disruption on the Assembly Line," reprinted from Stanley Aronowitz, *False Promises: The Shaping of American Working Class Consciousness*, New York: McGraw-Hill, 1974. pp.21-27.

⁷ Nuclear security involves protecting the missiles from unintentional launches, while nuclear surety ensures it is possible to reliably launch the missiles when directed.

determine “the best of the best” in exercises, readiness, and launch drills. The higher authority centralized control combined with the simultaneous multiple execution of events provide the safety necessary for nuclear weapons. Because of the risk associated with nuclear weapons, this process has remained relatively unchanged throughout the decades.

In the late-1980s, however, the missile crews asked that the computers in the silos have additional capabilities similar to personal computers so they could write papers for their Master’s degree while monitoring the missiles. This request was obviously disapproved. Computers that control nuclear weapons were not to be used for any other purpose.⁸

4. Vietnam and the Raid on Son Tay

While appropriate for the Cold War scenario, the decision and response time for other operations was unacceptably slow and tactically harmful. Vietnam was a centrally controlled war; yet, except for the bombing of the North during the Linebacker operations, the majority of sorties flown were of limited value. Pilots did not understand the significance of their mission. There was a lack of trust between the tactical operators and the strategic mission planners. Mission details from high-level command centers (even as high as the White House) included not only target information, but also specific routes, altitudes, and formations. Because North Vietnam had an effective air defense system, these missions took a heavy toll on U.S. aircrews.

A striking example of a failed operation because of this centralized decision-making process was the raid on Son Tay.⁹ In May of 1970, an SR-71 blackbird aircraft flying over Vietnam discovered a prisoner of war (POW) camp named Son Tay approximately 23 miles from Hanoi. When word arrived in the United States a team of Army Special Forces was assembled to rescue the prisoners. Colonel “Bull” Simons

⁸ As the software project manager for the program titled “Rapid Execution And Combat Targeting (REACT),” I was responsible for ensuring operational requirements were met while upgrading the command and control computer system for Minuteman and Peacekeeper ICBMs.

⁹ Specific details come from <http://www.psywarrior.com/sontay.html>, 26 October 2004

headed up the team of one hundred men to train for this rescue mission. They created a full scale replica of the compound and trained at night to ensure secrecy from Soviet satellites. When the final assault took place, 56 men were selected for the mission. Not until they were on their way did Bull Simons actually tell them what their mission was. Just after 11:00 PM the helicopters and C-130 combat talon took flight for the rescue mission. At the same time, the U.S. Air Force and Navy began several diversionary attacks to provide cover for the raid. The Son Tay raiders conducted a nearly flawless tactical raid and rescue mission except for one major problem – they conducted this raid on 18 November 1970, nearly six months after the initial intelligence arrived. After arriving at the camp and killing the North Vietnamese guards, they discovered there were no prisoners left in the camp. All prisoners had been moved in July. With the 1970s centralized decision-making processes in place, execution was slowed to such an unacceptable speed that the Special Forces team risked their lives to raid an empty prison camp.

C. The 1980s

1. Industry in The 1980s

In the 1980s, the personal computer (PC) revolution not only affected the way we use computers, but also reshaped how commercial industry and government operated. The 1980s marked the beginning of the small business boom. Steve Jobs and Steve Wozniak, founders of Apple Computer Company, invented the first easy-to-use microcomputer circuit board design for personal home use in 1976.¹⁰ Seeing the benefit, IBM quickly jumped on the new market possibilities, introducing the PC as a business machine in 1981. Soon after, Apple introduced the MacIntosh in 1984, creating a user-friendly interface for word processing and accounting. Equipped with a small computer, telephone, and fax machine, home offices sprang up as people ran their businesses in their living room.

¹⁰ Actually, this first Apple 1 consisted of only the circuit board. The buyer had to build his own box to install and make his own “home-brewed” computer. <http://www.apple-history.com/frames/> 6 December 2004.

Not everybody quit his or her job. Big businesses still employed the majority of workers; however, large companies, such as GM and Chrysler, had to revitalize the organizations to regain their competitive edge. Business practices changed dramatically as hundreds of new-style management books and articles gave advice to company CEOs (there was only one accepted style of leadership for large corporations prior to 1980).¹¹ Many professed the creation of vision and mission statements, worker empowerment, and total quality management. One powerful CEO, Sanford McDonnell of McDonnell-Douglas Aircraft Company, realized in 1982 that his company lacked a code of ethics in its vision statement. He assembled an executive task force to create one, the result of which looked very similar to the Boy Scout Law.¹² These are elements of establishing an environment receptive of influence and trust.

In a 1984 article, Noel Tichy and David Ulrich called for a “new brand of leadership” and dubbed visionaries like Lee Iacocca “transformational leaders.”¹³ What these leaders did was adjust their management style to influence the employees, empower key management factions, and create a new culture where employees were committed to work hard. When Lee Iacocca took over Chrysler, his first step was to create a vision statement. He then mobilized his managers to spread the philosophy and work ethic of the company, turning the vision into action. Finally, he institutionalized the change, creating a new culture for the work force. This soft-power leadership style is exactly what was needed in the 1980s for companies to be competitive. By 1984, Iacocca had brought Chrysler from the brink of bankruptcy to record profits.

2. The 1980s Military

Military organizations followed the same trends as their commercial counterparts in the 1980s. Leaders in the eighties who were junior officers during the Vietnam War

¹¹ Frederick Taylor’s “Scientific Management” method had been the accepted standard for running business since the 1900’s.

¹² Kidder, Rushworth, *How Good People Make Tough Choices*, New York: Morrow, 1995. p. 83.

¹³ Tichy, Noel and David Ulrich, “SMR Forum: The Leadership Challenge – A Call for the Transformational Leader.” *Sloan Management Review*, Fall 1984. Vol. 26. p. 59.

made sure that "decentralized execution" became the mantra of the tactical air force. Leaders talked about empowerment while squadrons developed new tactics, techniques, and procedures. Most of the training following Vietnam concentrated on solving the tactical problems encountered during the war. During the 1980s, U.S. airmen became highly proficient at air-to-air combat skills and attacking surface-to-air missiles (SAMs). A quick review of the *USAF Fighter Weapons Review* journals of the 1980s showed the emphasis on techniques to improve specific skills or capabilities of new missiles. There was little to no talk about command and control at the operational or strategic level. In fact, the journal was published by the USAF "Fighter" Weapons School and was specifically about fighter aircraft tactics only. It was not until 1992 that they dropped the term "fighter" from the school name as they expanded their scope and consolidated both operational and tactical mission training.¹⁴

Significant advancements in weapons technology were developed and fielded in the 1980s. For example, the F-16 community installed software upgradeable avionics computers and the first operational digital flight control system. This led the way to significant capability improvements such as flying low-altitude under-the-weather at night and employing precision guided munitions. Airframes became highly capable individual platforms (like the PC of the same decade), but were not interconnected with other systems, even aircraft of the same type. Emphasis was placed on making individual platforms as powerful as possible with the most highly trained aircrew available. "Smart" aircraft, like the F-16 and F-18, could handle any threat in the air or on the ground, even if outnumbered. However, little consideration was given to how the tactical mission fit into the overall plan.

Moreover, limited communications outside of organizational boundaries reduced the ability to share tactics and practice large force operational scenarios. Military plans called for deconflicting assets; as long as units operated separately, they could accomplish their mission. A perfect example of this was the success of Operation El

¹⁴ From a 1995 article by Eric Hehs in Code One Magazine, "USAF Weapons School Training Weapon Officers at Nellis AFB, NV," April 1995.
http://www.codeonemagazine.com/archives/1995/articles/apr_95/apr1a_95.html 1 December 2004.

Dorado Canyon over Libya. On the other hand, accomplishing the mission in scenarios that required integration and synchronization with other units proved to be extremely difficult, as was demonstrated in the failed Iranian Hostage Rescue.

3. The Libya Bombing

The 1986 bombing in Libya epitomizes the success of the 1980s military organization, force structure, and decision-making. Operation El Dorado Canyon, conducted on 15 April 1986 was in response to a terrorist bombing at a Berlin discotheque ten days prior.¹⁵ Almost 100 aircraft were deployed for the twelve-minute precision bombing of five targets. Although at first study this attack may appear to be a centrally organized, complex, joint mission, in reality it was a case of decentralized organizations, planning, and execution. Once the targets were approved by President Reagan, only the time and place required strict coordination. Actual execution was operationally and geographically divided between the services. The U.S. Air Force fighter-bomber and tanker fleet took off from England together (C2 for the Air Force was maintained on a modified tanker) while the Navy aircraft carriers took care of their own C2, electronic warfare, and air defense. The two services deconflicted their operations by airspace; the Navy aircraft were assigned targets in the Benghazi area while the Air Force hit targets near Tripoli. Essentially, two different operations were executed on the same night by two separate organizations by coordinating only the objective and the time on target. Each organization was free to conduct the operation as they saw fit.

Unfortunately, not all operations were planned with the concept of simple, separate deconfliction in mind. When complex synchronization was required, small units were not trained, equipped, or in the mindset to work together. This was all too apparent in the aftermath of the aborted Iranian hostage rescue mission of 1980.

¹⁵ Specific details come from http://www.globalsecurity.org/military/ops/el_dorado_canyon.htm, 26 Oct 2004.

4. Desert One, The Iran Hostage Rescue Fiasco

Unlike the Libya raid, the Iranian hostage rescue attempt was truly a joint complex endeavor. Unfortunately, the characteristic lack of connectivity of the 1980s model did not allow for this type of joint operation to achieve success.¹⁶

For this rescue mission, an ad hoc group was thrown together which included: Delta Force; Army airborne rangers; Air Force gunships and transport aircraft; Marine, Air Force, and Navy pilots; and Navy minesweeper helicopters. Every service needed to be a part of the operation. However, the chain of command was not clear. Most of these people had never worked together. The pilots chosen for the mission had no experience in long-range low-level flight with night vision equipment.

Trust and confidence was missing from the team. Delta Force members expressed a lack of confidence in the helicopter pilots. The pilots, unfamiliar with some of the aircraft avionics, expressed low confidence in the equipment. The planners enforced strict compartmentalization keeping organizations separate. They asked the CIA for intelligence support, but did not trust their information. Although they were given the exact location of the hostages in the embassy, they did not trust the source, and, therefore, would not reduce the size or footprint of the team.

The plan was extremely complex, required multiple synchronizations, and lasted over 40 hours. Even so, there were no full-scale mission rehearsals. There were no coordinated briefings or debriefings during the spin-up phase. Organizations simply did not work together. Sharing information was kept to a minimum. Helicopter pilots were not informed about the dust storm hazards, misinformed about their altitude requirements to hide from Iranian radar, and not given pilot reports (from the C-130s) about weather conditions ahead.

Historians have labeled the final execution of this rescue attempt a total fiasco. On 24 April 1980, the helicopters and C-130s headed to Desert One, the rally point

¹⁶ Specific details come from Vandenbroucke, Lucien S., *Perilous Options*, Oxford University Press, 1993, pp. 121-151.

before the raid. However, dust storms, misinformation, lack of communication, and aircraft maintenance problems led to several helicopters aborting prior to arrival at Desert One. President Carter approved the recommendation to abort the mission due to lack of required helicopters. When the aircraft began departing for their return, one helicopter pilot became disoriented and crashed into a C-130, exploding both aircraft and the ammunition onboard, and killing eight crewmembers.

Overall, this operation failed for reasons besides bad luck. Instead of being a cohesive team, the separate organizations did not share knowledge or communications. The common characteristic among the entities was lack of trust. The required synchronization to handle the complexity of the mission was nonexistent.

D. The 1990s

1. Industry in The 1990s

With the 1990s came the advent of the local area network – and commercial industry followed suit. This was the decade of consolidators. Hometown retail stores went out of business as large companies gobbled up small businesses. Superstores such as Target and Wal-Mart created an environment where shoppers could buy everything they needed under one roof. Prices for individual items dropped dramatically as the efficiency of the operations increased. These consolidated superstores created an efficient and effective commercial industry for themselves.

The retail industry was not alone in this phenomenon. When Boeing and McDonnell Douglas announced its merger in 1997, “synergy opportunity teams” formed to identify the best practices within the groups and then share them company-wide. Creating “one company” was the number-one priority. In 1995, Kraft Foods reorganized into a single operating company and followed a management change regiment to identify necessary elements that would contribute to the new leadership vision.¹⁷ This differed

¹⁷ Carter, Louis, David Giber, and Marshall Goldsmith, *Best Practices in Organization Development and Change*. Linkage Inc., New York: Jossey-Bass/Pheiffer, 2001. pp. 12, 193.

from the 1970s because lower level managers were allowed to have input into the consolidation efforts.

Although power was amassed at the top, lower level teams were still allowed to think of tactics to increase efficiency of operations. During Boeing's 777 project in 1994, rather than structuring the organization with the typical management hierarchy, instead Boeing organized into a hierarchy of teams. Top management was kept well-informed in order to make quick decisions.

Unfortunately, while within the organization there was connectivity and shared knowledge, separate organizations were still not practiced at communicating with one another. Wide area networks and the internet were still in their infancy and communication lines were slow. Management had to form integration teams and insist they had access to everyone in the organization. These cross-functional teams passed information both horizontally and vertically, thereby sharing important integration data quickly and efficiently. The result was the Boeing 777 flew its first flight with less than half the usual number of design glitches compared to past aircraft.¹⁸

2. The 1990s Military

As networking technology was incorporated into military systems, commands were able to focus on synchronizing operations, not just tactics of individual platforms. Strike packages included all assets from bombers, counter-air fighters, electronic warfare jammers, tankers, JSTARS, and AWACS. The Powell doctrine advocated using large groups of overwhelming force to encounter any contingency.

Leaders reined in the decentralized "cowboy" decision-makers back under the control of a hierarchical commander. The new organization was federated, but closely monitored – sometimes too closely monitored. The command and control platforms of the strike packages maintained constant communications links with the Combined Air Operations Center (CAOC). The operations floor of the CAOC took on a whole new

¹⁸ Szewczak, Edward, *The Human Side of Information Technology Management*. Pennsylvania: Idea Group Publishing. 1996. pp. 182-183.

mission, as they were able to pull information from all sources together to identify and direct precise attacks on fleeting or time sensitive targets. The process included the following steps: find, fix, track, target, engage, and assess (F2T2EA). Prior to advanced automated networking, a commander had to communicate clearly his intent and trust his subordinates would carry out his orders to the best of their abilities. With their newly found real-time situational awareness, upper echelon leaders could track all engagements and provide immediate direction. Sensitive to strategic consequences, the commander in the CAOC could not only plan the operations, but also direct the specific tactics for precise effects.

With the battlefield debut of Predator unmanned aerial vehicles (UAVs) in Operation Allied Force, the CAOC gained “eyes on” the targets, albeit through a soda straw. There are several accounts where experienced tactical fighter pilots returned to base with unexpended ordnance, thoroughly frustrated with the CAOC delaying attack authorization. Even when the rules of engagement cleared the pilot to attack, the CAOC would wait for the Predator to fly (at only 100 mph) to their location to see the target for themselves. Because of political sensitivities, the commander deemed the risk too high to trust the pilots with the decision to engage.¹⁹ When discussing these operations, one experienced fighter pilot from the 1980s-generation commented on the centralization of power to the CAOC, “Now all you need is a monkey to fly jets – to fling poo and pickle JDAMs.”²⁰

Aside from the frustration among the subordinates, Operation Allied Force was considered a success. Other operations, such as Operation Desert Storm, were considered a glowing success because of the synergy created by the 90s-style organizations being combined for strategic effects.

¹⁹ Several excellent examples are given in Major Douglas Nikolai’s thesis titled “Centralized Execution of USAF Air and Space Forces: The Unspoken Trend of the Master Tenet,” Naval Postgraduate School, September 2004.

²⁰ Personal interview with anonymous fighter pilot. Officers Club, Nellis AFB, NV. 30 July 2004. This source had over 20 years flying experience. The term “pickle” refers to hitting the release button for a bomb. JDAM is a GPS-guided “smart” bomb.

3. Desert Storm

The technology and tactics that developed in the eighties were demonstrated on a large scale in 1991 when the United States and coalition partners began the air war over Iraq.²¹ Using state-of-the-art precision guided munitions, contemporary blitzkrieg tactics, and ultramodern electronic jamming pods, U.S. forces waged an entire war in 43 days. However, while the operation was lauded as a joint success, the different services were almost always separated by time and space.

The campaign was split into four phases. Phase 1 consisted of gaining air supremacy and breaking Iraqi command and control. Tomahawk missiles and strategic air assets accomplished this mission. Phase 2 was aimed at destroying Iraq's ability to wage war. This was an aerial bombing campaign targeting weapons of mass destruction, Republican Guard divisions, and oil refineries. Phase 3 was a third aerial campaign to attack occupied Kuwaiti bases and demoralize the troops. Finally, Phase 4 was the ground war. Even in this case, Army divisions executed the famous "left hook" crossing the Saudi Arabia-Iraq border while Marines provided a decoy in the east.

By planning and executing the war in phases, large homogeneous forces could accomplish their mission while still remaining deconflicted from other organizations actions. General Schwarzkopf centrally controlled the timing several hundred miles away in Riyadh, Saudi Arabia.

4. Somalia

Unfortunately, American soldiers were not so lucky when they were ambushed by an angry swarm of gunmen on the streets in Mogadishu, Somalia.²² The film "Blackhawk Down" graphically portrayed the terrible outcome of centralized control leading to disjointed communications in the 1990s.

²¹ Desert Storm details come from Builder, Banks, and Nordin, *Command Concepts: A Theory Derived From the Practice of Command and Control*. RAND, 1999. pp. 55-72.

²² Information about the raid in Somalia comes from Sean J. A. Edwards *Swarming on the Battlefield: Past, Present, and Future*. RAND, 2000. pp. 46-52.

On 3 October 1993, U.S. Rangers and Delta Force Teams fast-roped into a gathering of Habr Gidr clan leaders to capture some of Mohamed Aidede's top men. Once captured, humvees were to collect everyone and drive them back to their beach camp. However, during the egress, two Blackhawk helicopters were shot down by rocket-propelled grenades (RPGs) just a few blocks away from the raid. A third team fast-roped in to secure the first crash site while the convoy holding the Somali captives was sent to secure the second crash site. However, the convoy never found it. Instead the humvee convoy wandered aimlessly through the streets in search of the crash while continuously being bombarded with gunfire at every intersection.

How could this happen to such a well-equipped, well-trained force? Sean J.A. Edwards of the RAND Corporation explains:

The U.S. situational awareness was poor. Although officers circling above in command helicopters had access to real-time video during the firefight, the video did not properly communicate the raw terror and desperation of the situation on the ground. Naval reconnaissance aircraft had no direct line of communication with the convoys on the ground. The Orion pilots were not allowed to communicate directly with the convoy. Their orders were to relay all communications to the Joint Operations Center (JOC) back at the beach. Also, no direct radio communications existed between the Delta Force ground commander and the Ranger ground commander. Their attempts to guide the wandering line of vehicles toward the helicopter crash site failed because of the delay in relaying directions to the ground commander.²³

Because of the pre-established rules to create centralized command and control, different organizations were not set up to directly communicate with each other even though the teams were in the same vicinity and could have supported one another. Instead, communications paths were designed to ensure deconfliction among the separate organizations rather than synchronization. The communication bottleneck at the JOC lead to confusion at the front. When the forty-hour battle finally ended, 18 American soldiers were dead. Soon after, President Clinton announced the immediate withdrawal of U.S. troops in Somalia.

²³ Edwards, *Swarming on the Battlefield: Past, Present, and Future*. RAND, 2000, p.51.

E. The 2000s

1. Industry in The 2000s

In the 21st century, the internet and intranets provide access to information for the masses. Just as important as receiving information, individuals can now transmit it also. The internet allows individuals to broadcast their message to a worldwide audience. Small groups that had previously remained separated due to geography can now interact with ease. Limitations from the cost of telecommunications or bandwidth disappear as new avenues to share information are created such as DSL, cable modems, and WiFi. What we gain is exponential growth as virtual communities and markets materialize with ease on the net.

eBay is an example of a company that has taken advantage of our new networking capability. On eBay, thousands of virtual relationships are formed simultaneously. Individuals decide with whom they want to communicate and conduct business. Since there is no need for a centralized source to approve decisions at the individual level, these transactions can occur through mutual synchronization of the sellers and consumers without the final decision being made by eBay. In fact, eBay does not care what the transaction was or who sold the item, they just insist that the virtual interactions follow the rules of engagement that eBay institutionalized. They also expect to collect their commission for each sale. The “command intent” is clearly recognized by all the participants

Besides providing the venue for e-commerce, eBay has created an innovative method for assessing trust across the computer screen. Through an eBay score, buyers and sellers build a reputation based on feedback from past sales. At the conclusion of each transaction, members are asked to rate the other’s performance. Sellers with consistently good ratings earn the honor of “power seller.” These ratings allow buyers to be more confident when bidding on an item, which in turn, increases the overall number of transactions on eBay.

Google is another company that is profiting from this information revolution. Because of Google’s innovative search and filter capabilities, it is relatively simple to

gain access to the specific information any user needs. This ease of accessibility makes it the number-one rated search engine in the world. Google has developed a method to display the best advertisements for a specific target audience depending on search criteria. In this way, consumers are comfortable receiving sponsored links along with their search results and continue to use Google as their primary search engine. Meanwhile, Google earns money from the advertisers each time someone clicks on one of their links. Access to the “correct” information for every individual is vital for organizations to function in the 2000s decade of the communication technology model.

2. The 2000s Military

Military organizations can share information making it possible for decision-making to occur at all levels within the chain of command. Thanks to the web structure, multiple redundant paths for information sharing are possible. Decision-making can become decentralized and no longer have to occur in series. But decentralization in the 21st century is different from that of the 1980s. Because of the power of networks, lower echelon troops have access to the information to make better decisions. With high quality information, competent troops, trust in operations, and a clear understanding of command intent, it is possible to empower subordinates with greater decision-making responsibilities than ever before. This is the aim of Network Centric Warfare (NCW) self-synchronization as originally envisioned by Admiral Cebrowski, the father of NCW.²⁴ This exponentially increases the speed of operations by increasing both efficiency and effectiveness.

3. Operations Enduring and Iraqi Freedom

Battles in the networked information age can be as geographically dispersed as the networks themselves. In Afghanistan and Western Iraq, there was no forward edge of the battle area (FEBA) or forward line of troops (FLOT). Instead, the battlespace was peppered with activity as it sprung up. Emerging targets of opportunity did not last long.

²⁴ Network Centric Warfare and Self-Synchronization are explained in detail in the next chapter.

Therefore, the standard operating procedures of the 3-day Air Tasking Order cycle were not acceptable, nor could the geospatial deconfliction of the past be used to conduct these types of operations. The data-linked information that provided a common operating picture for all services, however, allowed joint operations to occur simultaneously in the same space. In fact, truly joint operations occurred where these separate organizations had failed to operate jointly in the past.

In Afghanistan, Special Forces teams traveled on horseback, searching through caves for Taliban operatives. As needed, the teams would call in air power to drop precision guided bombs at the determined coordinates. While close air support has always been part of Air Force-Army doctrine, never before had it been done with a B-52 strategic bomber matched up with small ground teams. Because the targets were fleeting and the best sensors were the SF teams themselves, the Air Force tasked bombers directly over to Army control rather than approving each bomb drop through the CAOC. This process formed the template for the concept of operations in Iraq's western war.

Over the western desert of Iraq, well-trained, well-equipped task forces teamed up with data-linked aircrews to conduct a SCUD hunt across 100,000 square miles. Because the strategic and political consequences of a SCUD hitting Israel, it was of utmost importance to find and stop any SCUD before it launched. Bomb release authority was pushed down to the lowest level to ensure a timely engagement. The CAOC in this case helped, rather than hindered, the aircrews by pushing forward target information that was compiled by networking sensors in the CAOC. Because of clear rules of engagement, experienced crews, and shared situational awareness brought about by the network, this decentralized mission was a great success.

4. OIF2 Abu Ghraib Prison

The key to successful decentralized decision-making is the ability to trust subordinates. With easy access to the information they need, they can make their own decisions, and then have the power to send information anywhere. At any level of command, individuals can receive information, decide on an action, and transmit knowledge.

Unfortunately, inappropriate incidents that occurred during the stabilization phase of Operation Iraqi Freedom have caused not just strategic consequences, but political and diplomatic consequences as well. The prison scandal that occurred at Abu Ghraib was a major setback to American credibility in Iraq and around the world.

The nature of stability operations requires the coordination of multiple organizations performing a spectrum of tasks from providing medical aid and rebuilding universities, to capturing insurgents and securing prisons. It would be extremely difficult to centrally control the myriad of tasks required to rebuild a nation. Therefore, decentralization is required for these operations. However, for decentralization to work, a commander must have competent troops that he trusts to follow the intent of his orders in an ethical manner. At the Abu Ghraib prison, that did not occur. Guards treated prisoners in such an abusive manner that many people around the world considered the events to be torture – and the guards took pictures. With easy access to multiple paths of communication, these digital images were passed electronically to the media, leading to the prisoner abuse scandal. What this shows is that in the 21st century, a soldier at any level of command has power to affect outcomes by having access to communication media. Since shared knowledge and accessibility to information are such critical factors to good decentralized decision-making, it is very difficult to control or stop information flow. This event also shows the importance of influencing the troops to think critically and act ethically to meet the intent of the mission.

F. Is The Military Stuck in the 1990s?

According to the model, we should be well in the middle of a period of decentralization. Yet, as we enter 2005, the military has not adopted the model for the 21st century except in some isolated cases. Why is that? Could the model be wrong? My answer is that the model is correct – the military is just behind. The problem the military faces is that it is still stuck in the nineties. This could be due to several reasons. Here are three possibilities for the delay in transformation. These are not being submitted as the explicit causes for the delay; they are just a few of several possible reasons to consider.

1. Reduction of Military Research and Development

Military research and development (R&D) was scaled back at the end of the Cold War. Government R&D requires a several year lead-cycle before the products make it to the field. What that implies is that items that were developed in the 1980s become operational in the 1990s, and innovations of the 1990s do not become useful until the 21st century. When the Cold War ended in 1991, however, military R&D sustained major funding cutbacks. In the 1992 State of the Union address, President George H.W. Bush declared: “By the grace of God, America won the Cold War.” He continued:

Two years ago, I began planning cuts in military spending that reflected the changes of the new era. But now, this year, with imperial communism gone, that process can be accelerated.... After completing 20 planes for which we have begun procurement, we will shut down further production of the B - 2 bombers. We will cancel the small ICBM program. We will cease production of new warheads for our sea-based ballistic missiles. We will stop all new production of the Peacekeeper missile. And we will not purchase any more advanced cruise missiles.... The Secretary of Defense recommended these cuts after consultation with the Joint Chiefs of Staff. And I make them with confidence.... The reductions I have approved will save us an additional \$50 billion over the next 5 years. By 1997, we will have cut defense by 30 percent since I took office.²⁵

This marks just the beginning of the defense budget cuts of the 1990s. Under the Clinton administration, the United States focus shifted to global trade and the economy. While in past decades commercial industry would spin-off ideas from military technology, now there is a paradigm shift where the military searches for commercial off-the-shelf technology (COTS) to advance military systems.

2. Military Downsizing

Military downsizing in the 1990s led to a smaller pool of innovative thinkers. The reduction in force (RIF) between 1992 and 1999 brought the active duty military end strength down from almost 2.2 million to under 1.3 million servicemen – a 36% cut in

²⁵ President George H.W. Bush's Address Before A Joint Session Of The Congress On The State Of The Union. January 28, 1992. Reprinted on C-SPAN.org.
http://www.c-span.org/executive/transcript.asp?cat=current_event&code=bush_admin&year=1992

total force. In addition, DoD civilians were cut by 34%.²⁶ There was simply a smaller pool of personnel to generate innovative ideas. Moreover, the personnel that remained spent much of their time figuring out how to keep doing the same mission with fewer people. The standard line: “We have to do more with less.”

3. Counterintuitive to Military Mindset

Distributing power and control across a network is counterintuitive to the military mindset. From the first days of basic training, soldiers learn to follow orders and never jump the chain of command. A hierarchical force structure is the paramount of classical military organization. This comes from the premise that not following orders can get you killed, or even worse, sacrifice the mission. Generals and Admirals have been promoted to their current positions because of their demonstrated ability to effectively command subordinates. Military leadership expects to maintain the classical architecture that has been engrained in their culture since the Roman Empire.

For example, the next chapter examines the debate over the best use of network centric warfare. The originators of the concept believed it would lead to decentralization and a distribution of control. However, the military leaders have used its networking capability to centralize decision-making and increase control. This will not last as lower echelon troops gain access to more information. The additional knowledge and situational awareness will embolden them to make their own decisions. Unless information is strictly controlled and/or denied, centralized commanders will have little power to stop this from occurring. Instead leaders must get ready for the change in the next generation of warfighters by figuring out how to use soft power – how to project influence and build operational trust.

G. Evidence We Are On Our Way

There are several cases where progress is occurring in the direction of the CommTech Model of the 21st century. For example, because of the emphasis on

²⁶ The FY 1999 Defense Budget And Future Years Defense Program, Chapter 21. <http://www.defenselink.mil/execsec/adr98/chap21.html>. 6 December 2004.

coalitions and the necessity to conduct military operations other than war, the Joint Requirements Oversight Council (JROC) has proposed changing the Joint Publication's Principles of War to replace Unity of Command with Unity of Effort. This is in response to the "evolving fundamentals of 21st century joint warfare and crisis resolution."²⁷

Another example is the number of non-certified networking technologies that show up and are immediately integrated into operations. These relatively inexpensive "garage projects" do not follow the normal programmatic acquisition and budgeting cycle restraints. Instead, units salivating for the new equipment will not wait for the programmatic bureaucracy to incorporate new capabilities.

A recent action by the Marines in Fallujah is one of the most telling stories of the change towards network organizations that cannot be stopped. In May 2004, during the height of the uprising in Fallujah, Iraq, ABC News reported a story about a Marine company in Fallujah taking matters of communications into their own hands. According to ABC, this company of marines determined they needed communications among all team members to fight in an urban environment. Pentagon leaders had withheld radios from the lower ranks due to concerns with radio bandwidth overload and security. The commander suggested that each soldier email home to ask for Motorola Talkabout radios. One marine's mother, a waitress in Texas, collected \$8000 from patrons and went to RadioShack to buy the Talkabout radios for the entire company. This is another example where if asking up the chain for communications support was getting "shot down" (so to speak), then they would solve their requirements by other means.²⁸

H. Summary

The CommTech Model provides the past explanation, current trends, and future direction for organizations, leadership style, and decision-making processes. With the exponential growth of networking capabilities in the 21st century, everyone will have

²⁷ JROC Memorandum 022-03, "An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution in the 21st Century." Directorate for Operational Plans and Joint Force Development, Joint Staff, 28 January 2003.

²⁸ ABCNews.Com. "Priority Mail: Determined Mom Helps Soldier Son Fighting in Iraq" By Mike von Fremd. Mansfield, Texas. May 19, 2004.

much greater access to information. Knowledgeable individuals within organizations will want to be the decision-makers. The military is no exception. As the military forges new paths implementing the concepts of network centric warfare and network enabled operations, several issues will arise affecting leadership, doctrine, force structure, and command and control. Under this premise, the debate has begun.

CHAPTER 3. UNDERSTANDING NETWORK CENTRIC WARFARE, SELF-SYNCHRONIZATION, AND NETWORK ENABLED OPERATIONS

A. *Introduction*

In a United States Naval Institute *Proceedings* Article in January 1998, Vice Admiral Arthur Cebrowski and Mr. John Gartska introduced the concept of Network Centric Warfare (NCW) with the following statement:

We are in the midst of a revolution in military affairs (RMA) unlike any seen since the Napoleonic Age, when France transformed warfare with the concept of levee en masse. Chief of Naval Operations Admiral Jay Johnson has called it a fundamental shift from what we call platform-centric warfare to something called network-centric warfare,” and it will prove to be the most important RMA in the past 200 years.²⁹

Six years and numerous books, articles, and speeches later, the original NCW concept is still poorly understood by the general military audience. Defining the specifics of the concept is not an easy task. Leading experts of NCW are still grappling for the right words to describe them, but have yet to reach a consensus.

A fallout of this is a misunderstanding by the larger general audience when it comes to “operationalizing” the concept. This leads to the big debate. While there is a consensus on the inherent benefit of exploiting information technology, the opinions of *how* the command structure should change are often diametrically opposed. Both camps proclaim they follow NCW principles. What this chapter shows is that the differences between the two approaches reflect the changing aspects of the 1990s and 2000s decades in the CommTech Model presented in Chapter 1.

This chapter introduces the debate between centralized and decentralized decision-making with respect to networked operations. After explaining network centric warfare basic principles, it will present the second-generation concept, self-synchronization, and the future vision, network enabled operations. With a common

²⁹ Vice Admiral Arthur K. Cebrowski and John Gartska, “Network-Centric Warfare: Its Origin and Future,” *Proceedings*. U.S. Naval Institute, January 1998. Vol. 124, Issue 1, pg 28.

understanding of these military concepts, the military will be able to specifically address the leadership styles and decision-making strategies of the present and future as they relate to networked organizations. Finally, this chapter raises current issues related to network enterprises.

B. The Debate

Two command and control approaches are developing in which both sides believe they are employing exactly what is meant by NCW, even though their approaches are diametrically opposed. Military leaders sponsor new technology experiments that centralize control to increase precision, reduce error, and orchestrate synchronized strategic effects. Meanwhile, leading Department of Defense civilian authorities advocate that a decentralized control system can exponentially increase the operational tempo without discarding the other benefits.

Military commanders in the Combined Air Operations Center (CAOC) applaud the advances in information technology that have improved their battlespace situational awareness. Lt Gen T. Michael Moseley, the Combined Force Air Component Commander (CFACC) in the CAOC at the beginning of Operation Iraqi Freedom, said in an interview following the war, “The CAOC is a weapon system in itself. When you have an organized structure, you have it manned right, and you have it equipped right, then it is an extremely lethal weapon.”³⁰ The common operating picture projected on giant screens over the CAOC main floor greatly enhanced decision-making for synchronized operations. The Air Force Doctrine Document 1 asserts, “There may be valid reasons for the execution of specific operations at higher levels, most notably when the Joint Forces Commander (or perhaps even higher authorities) may wish to control strategic effects, even at the sacrifice of tactical efficiency.”³¹

Initiatives such as Network Centric Collaborative Targeting (NCCT) at Joint Expeditionary Force Experiment (JEFX) 2004 demonstrated the capabilities that NCW brings to centralized decision-making. The NCCT network used machine-to-machine

³⁰ Kunz, Christine L., “OIF info 'brain'” *Airman*. Oct 2003. Military Module, pg. 22

³¹ Air Force Doctrine Document 1. Department of the Air Force. 17 November 2003. p. 30.

cross-cueing to collaborate information from multiple sensors. This provided the Combined Force Air Component Commander (CFACC) with timely, target-quality information on high-priority targets and Time Sensitive Targets (TSTs).³²

The point the other side makes is, if this targeting information can be collaborated for the CFACC, then why not pass the information directly to the pilot who will actually drop the bombs? Is it necessary for the CFACC or higher authority to approve each target if it already meets the criteria pre-established in the command intent?

Advocates of decentralized control, including the Office of the Assistant Secretary of Defense (NII), believe that with increased knowledge and awareness by all entities, there is less need for a hierarchical command and control structure. As long as the commander's intent is well understood, lower echelon warfighters will make the correct decisions because of increased situational awareness (SA) and will act accordingly. Combining NCCT results with another JEFX system, Cursor-On-Target, enabled the exact target coordinates to be broadcast over the data link to all aircraft. Empowering the edge actors, such as forward-deployed strike packages, to make decisions and act will free up the general's time so he can focus on higher-level strategic issues.

Major Douglas "Stoli" Nikolai, a U.S. Air Force F-16 pilot who saw first-hand both approaches being executed at the CAOC during Operation Iraqi Freedom, sums up the argument well in his thesis published September 2004:

In general, decentralized execution capitalizes on initiative, flexibility, and situational awareness (SA) that normally are conducive to tactical effectiveness, efficiency, and mission success. On the other hand, centralized execution takes advantage of technology that allows high-level commanders to personally direct tactical level operations in an attempt to control strategic repercussions, which normally contributes to a loss of

³²The Joint Expeditionary Force Experiment (JEFX) Live-Fly was conducted in August 2004. Preliminary results are in "Joint Expeditionary Force Experiment 2004 Quicklook Results and Initial Recommendations," Air Force Experimentation Office. September 2004.

efficiency, inherent delays, frustration on the part of warfighters in the field, and decreased mission success.³³

The differences between these two command and control approaches beg for different terms. This first approach of centralized command and control may be called the first generation of network centric warfare, NCW (Basic). Whereas, the decentralized command and control approach should be considered the next generation of NCW, called Self-Synchronization. This leads to the future vision of networks, called Network Enabled Operations (NEO). As currently used by the defense community, these terms often overlap. However, this thesis makes a sharp distinction between them because the differences between NCW and Self-Synch/NEO reflect the same cycle between hard-line control and softer power illustrated by the CommTech Model.

C. The Basics of NCW

Network Centric Warfare is the concept of organizing and distributing critical, tactical information, via high-speed data links and networking software, to increase efficiency and effectiveness of military command and control. This awareness and knowledge is then leveraged to increase the efficiency and effectiveness of actions. NCW is more than just advanced data link systems – it requires the co-evolution of doctrine, concepts of operations, force structure, and tactics. Advocates predict it will improve combat power by increasing the speed of command, tempo of operations, lethality, and survivability.³⁴ Conceived in the 1990s, the decade of collaborating resources for increased synergy, NCW pulls information together to reduce uncertainty and increase confidence in decision-making, while bringing precision to execution.

³³ Nikolai, Douglas, Thesis: “Centralized Execution Of USAF Air And Space Forces: The Unspoken Trend Of The Master Tenet (Unclassified Version),” Naval Postgraduate School, Monterey, CA, September 2004. p. 4.

³⁴ David Alberts, John Garstka, and Frederick Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. C4ISR Cooperative Research Program (CCRP), Washington, D.C. 1999. p. 86.

The value of information is based on its accuracy, timeliness, and relevance at all stages of command and control. NCW strives to improve all three of these.³⁵ Increased capabilities in sensor performance and precision measurements provide better data upfront. With multiple sources collecting similar data, error ellipses can be reduced providing increased accuracy. Since information can move at the speed of light, once the information is processed, it can be distributed immediately, greatly improving the timeliness of the information. NCW provides decision-makers with a common operating picture, greatly increasing the situational awareness of everyone in the battlespace. Proper doctrine along with experience, education, and training can provide guidance for information analysts to correctly assess the relevance of the information. Having a common perspective and knowledge will facilitate our military forces in executing correct actions to achieve the commander's intent. The power in NCW lies in the synergy achieved by linking multiple entities to increase information superiority. Figure 3-1 illustrates the simplified process of this first-generation NCW command and control.

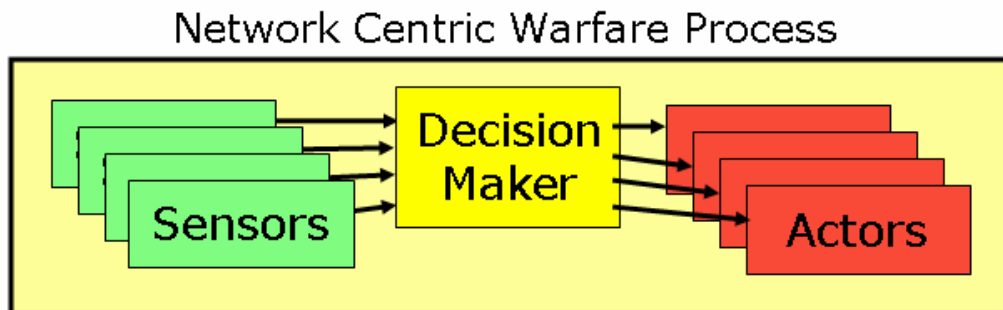


Figure 3-1. The Network Centric Warfare Process

There are three main types of entities, all of which can be improved through Information Technology (IT): sensors, decision makers, and actors. These entities have always been inherently linked to perform the mission. With information technology, we can network all of these entities, providing better results from each. The more sensors

³⁵ David Alberts, John Garstka, and Frederick Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. C4ISR Cooperative Research Program (CCRP), Washington, D.C. 1999.

that share information, the better the knowledge becomes. For example, a Joint Surveillance Target Attack Radar System (JSTARS) aircraft finds a potential target with its moving target indicator. Other sensor platforms discover through electronic signature that a surface to air missile (SAM) site is tracking friendly aircraft in that area. By sharing each other's information, they can merge the data to conclude there is a hostile SAM site at the given location. Through developments in IT, we can automate the fusion process and augment with multiple sensor sources to consolidate the target information more reliably. When the sum of this information is passed to the decision makers, inevitably they will make better decisions with a higher degree of confidence.

Armed with precise information, the actor can attack the target with increased probability of kill while minimizing personal risk. Continuing with the above example, an F-16 pilot will automatically have the consolidated target type and location information displayed in his cockpit. This enables him to choose the optimal attack tactic, weapon choice, and electronic warfare jamming profile in minimal time. He quickly destroys the target on his first run, with a single precision-guided bomb, and decreases his loiter time in the threat missile engagement zone. Machine-to-machine interfaces ensure there are no transcription errors when passing the data across platforms. Furthermore, planning and execution time can be reduced, enabling each actor to engage more targets. Only the beginnings of NCW are shown in this example. NCW will encompass both lower level tactics and higher level strategies. Therefore, it is important to understand some key concepts of NCW.

D. Key Concepts

Experts in NCW list three key concepts that should be emphasized when explaining the idea: 1) forces can be geographically dispersed; 2) troops are more knowledgeable; and 3) one can achieve effective linking among entities.³⁶

The first key concept is that forces can be geographically dispersed around the globe. Instead of the logistics of moving people and machinery to deployed locations,

³⁶ Alberts, Gartska, and Stein. *Network Centric Warfare*. pp. 88-93.

now we move information to the desired location. Using NCW techniques, the military can focus on delivering effective combat power – shooters, bombs, and bullets – to the theater instead of wasting limited assets, time, and money, moving everybody else that could just as easily do their job from their current location.

Thanks to militarized versions of internet protocol, chat rooms, and email, information can easily be shared in several locations at the same time. This reduces the constraint that everyone needs to be co-located in order to provide proper command and control. If the information is accessible in multiple locations, then fewer people have to forward-deploy during a contingency. Organizations that operate best in their permanent building due to equipment requirements can remain in place. For example, a satellite downlinks its sensor data to the ground station it is currently flying over. That data package is forwarded and processed using specialized supercomputers within the United States. The resulting information is then transmitted back to the Combined Air Operations Center (CAOC) in the deployed location. The deployed CAOC can have a smaller footprint because more assets can work from their home location. Additionally, if more assets are dispersed, the CAOC becomes a less attractive target for the enemy. Our command and control will be less vulnerable if the command and control functions are geographically dispersed.

The second key concept is that the troops are knowledgeable. With a clear understanding of the commander's intent and the information provided by the network, a lower echelon commander could better understand the execution orders and plan a more robust attack. Empowered forces can control their area of responsibility leaving the top-level commanders with time to deal with future issues instead of the issues at hand. The overall battle rhythm increases when the responsibility for tactical execution decisions is delegated to lower-level forces.

The third key concept is the one can achieve effective linking among entities. It is imperative to design a robust network architecture to ensure the information retains its accuracy, relevance, and timeliness throughout the network. All players must receive the necessary information in order to make suitable decisions and correctly interpret commands. Multiple redundant paths for communication are required to ensure the data

reaches the intended receiver. High quality information can improve all players' shared situational awareness, greatly reducing errors and uncertainties. Every subspecialty builds into the synergy created from joint and coalition forces. This can increase the precision and lethality of the force.

The benefits of these concepts were demonstrated at the Joint Combat Identification Evaluation Team (JCIET) Exercise 2002 through an experiment called "remote positive control" during a close air support (CAS) mission. The focus of the exercise was to assess ways to reduce fratricide without jeopardizing combat effectiveness. In the scenario, U.S. Air Force F-16 and A-10 aircraft provided CAS for an army tank battle. The difference in this experiment was that the ground forward air controller (FAC) was not out with the tanks. Instead, he was far behind the forward line of own troops (FLOT) in a tent with multiple computer displays. The friendly aircraft, ground vehicles, and FAC were all equipped with a data link providing each other's friendly position data, available weapons, course, speed, etc. The JSTARS downlink provided enemy tank locations. The FAC believed he had enough situational awareness, knowing where both the friendly forces and enemy forces were located, to direct the attack from his remote location. The data link allowed targeting information to go directly into the aircraft navigation systems, avoiding possible mistakes from transcribing coordinates. Since the aircraft cockpits were also equipped to display the same data-linked friendly and enemy locations, the pilot could quickly assess the information received and have confidence he was seeing the correct target, hence reducing the risk of fratricide. Furthermore, the FAC could see via data link where the aircraft was targeting, thus confirming his directions. Armed with this information the remote FAC could quickly clear the pilot for attack.

In this scenario, using NCW concepts, the FAC was able to control the aircraft in a less stressful environment with better collective information. The pilots could execute the attack knowing the location of all the friendly forces. Control was effective while being geographically dispersed. The speed of command was greatly increased as all players shared the same operational picture. Targeting information was automated,

reducing human errors. Overall, the risk of fratricide was reduced even though the FAC was not on location.

E. Methods of Information Sharing

With the synthesis of all this new information, the potential for information overload exists. A human can only process so much useful information. Who determines which information is useful and what is just noise?

One mechanism to address this issue is in the next generation data link networks currently being designed. These address the way we pass information. There are three type of information sharing methods easily named: 1) push, 2) smart push, and 3) post and pull. The first generation of data links uses the “push” method. In other words, everybody pushes all of their data to everyone else. This is similar to a broadcast message that goes to everybody in the network. There is no specific target audience. Bulk official email to everyone can be considered a pushed message. Another example is a generic chat room that everyone monitors and adds information. When trying to do this in the RF spectrum, frequency allocation becomes an issue. To save bandwidth, this data is often pushed in a time sharing manner. For example, in the Joint Tactical Information Distribution System (JTIDS) Link-16, everyone transmits their own position data, and command and control nodes such as AWACS or JSTARS push all of their surveillance data. The opportunity to transmit in the approximately 1500 timeslots over a twelve-second period is systematically distributed among net members. As the amount of data and the number of net members increase, however, it becomes difficult to get all the information to everyone within the allocated timeslot design. In addition, not all members care about everybody else’s information. For example, an A-10 pilot working directly with a ground team providing close air support in urban terrain does not care about the surveillance data being transmitted by an Aegis cruiser 300 miles away. Yet this information takes up valuable bandwidth that could better be utilized by faster update rates of data that is relevant to his mission. However, he may need the Aegis data when he is returning to his base on the coast.

The second method, “smart push,” addresses part of this problem. With smart push, data is directly transmitted, or pushed, only to the units that need it. For example, a C2 message such “Attack target #1234” will be pushed directly to the aircraft that is to execute the command. This is the mission equivalent of sending an instant message to someone or an email if the information is less time critical. Additionally, information can go to a specific group of members. For example, small subnets can form that share high-resolution mission specific data when necessary, such as a 4-ship of F-15s sharing target sorting data. This is similar to creating small “members only” chat rooms or holding meetings via teleconferencing. In addition, messages can be directed to a specific target audience, such as current threat data to all units in a geographic area, just as email can go to specific distribution lists. The main advantage of smart push is its ability to reduce information overload at the receiving end. Information must be relevant; otherwise, it becomes a distraction. Smart push helps reduce the barrage of useless information that clutter the displays and each person’s mind. The disadvantage with smart push is the owner of the information must know exactly who needs it. Also, depending on the RF data link design, even specifically addressed messages can use up valuable bandwidth.

The third method is the “post and pull” technique of moving data. In this approach, the information owner posts and updates his data to a specific location or website. Then, users decide what information is relevant and pull that data from the webpage when they need it. We use this everyday when we go to specific websites to check bank accounts, research topics, retrieve webmail, or buy online products. With the new system, the user will pull only the data needed, saving downloading time and avoiding clutter and confusion. To determine what each user, team, group, or platform wants will require excessive preparation. After all, “You don’t know what you don’t know, and they don’t know what you need to know.”³⁷

The demand for the right information at the right time drives the second-generation concept of network enterprises, called NCW Self-Synchronization. In a decentralized network environment, information is accessible to the authorized users

³⁷ Nicole’s quote. ☺

when needed. They are then able to make the right decisions based on command intent and their roles in the overall mission. Developing the rules for the proper mix of all three methods will require years of research and trials to optimize. As stated in the book, *Power to the Edge*, it will be critical to “provide necessary education and training to deal with the explosion of information.”³⁸

F. Transitioning to Self-Synchronization

As users share information and knowledge to make their own decisions and act, they perform Self-Synchronization – the NCW process conducted in a non-centralized manner. Self-synchronization is an effort to “increase freedom of low level forces to operate near-autonomously and re-task themselves through the exploitation of shared awareness and commander’s intent.”³⁹ In this approach, the knowledge is shared across the battlespace allowing multiple organizations on the edge of the command to be responsible for their own areas of expertise. These organizations that take these actions and effect change are considered “edge organizations,” because they reside on the edge of the normal command and control flow. This changes the dynamic of decision-making from a centralized to a decentralized process. When asked which is the priority, getting information to the CAOC or getting information to the fighters (or edges), Lt Gen Ron Keys, USAF, eloquently stated: “I think of it as information communism – each platform gives based on its capabilities and receives based on its needs.”⁴⁰

How self-synchronization works can best be explained by examining a decision process. Command and control has been based on decision loops such as John Boyd’s famous OODA loop – observe, orient, decide, act. The speed at which this cycle occurs affects the speed of command and ultimately the battle rhythm. With the goal of

³⁸ Alberts, David and Richard Hayes. *Power to the Edge*. C4ISR Cooperative Research Program (CCRP), Washington, D.C. 2003. p. 105.

³⁹ This definition comes from Rumsfeld, Donald H., *Transformational Planning Guidance*, Department of Defense. April 2003.

⁴⁰ Lt Gen Ron Keys, Deputy Chief of Staff for Air and Space Operations, Headquarters USAF. Interview Naval Postgraduate School, 24 August 2004. Lt Gen Keys has since been named Commander, Air Combat Command, USAF, beginning January 2005.

reducing the decision cycle time even further, self-synchronization comes into play. Actors at the edge of the organizations work with a shared knowledge, which provides them the ability to make proper decisions. By increasing the number of decision-makers, multiple OODA loops can occur in parallel.

When this process is turned into an operational flow, the sensor-to-shooter link becomes simplified and shorter, creating a significant increase in speed of action. This is the ultimate benefit of self-synchronization. Figure 3-2 illustrates the NCW changes between the first-generation NCW (Basic) and the second-generation NCW Self-Synchronization.

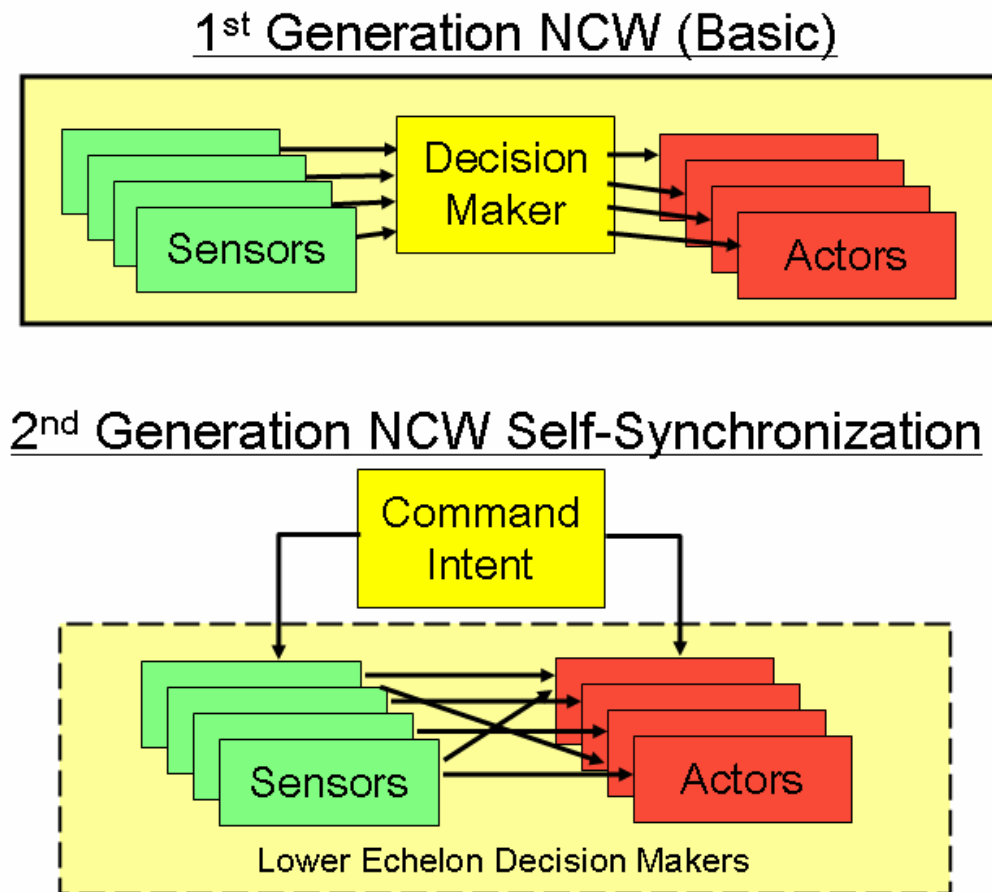


Figure 3-2. Comparison Between 1st and 2nd Generation Network Operations

For self-synchronization to work, four necessary conditions must be met.⁴¹ Without meeting these criteria, the full benefits of self-synchronization will not be realized. They are:

1. Trust in the information, subordinates, superiors, peers, and equipment;
2. Clear and consistent understanding of command intent;
3. High quality information and shared situational awareness; and
4. Competence at all levels of the force.

G. Envisioning Network Enabled Operations

Recently, concept engineers have been able to expand the singular concept of NCW into an even larger concept called Network Enabled Operations (NEO). By adapting the same basic principles as NCW, NEO expands the realm of networking beyond military command and control in warfare. Whereas, NCW began with a deconstructionist approach of examining every component and connection to increase effectiveness in war, NEO takes an expansionist approach increasing the breadth of opportunities to utilize networks. The concept of NEO asks how will networking be used in operations other than war, and how must we adapt our command and control doctrine to match this new environment? Using an analogy, if the NCW concept was comparable to studying the planet, NEO would equate to learning about the galaxy.

NEO shares the same tenets as NCW to include robust networks, information sharing, and mission synchronization. In NEO, however, the primary purpose of the network is to provide shared situational awareness to enable all organizations to make appropriate decisions. This differs from the way the military has implemented first generation NCW, where the emphasis of the network was meant to provide the actors with the information needed to execute assigned tasks.⁴²

⁴¹ Alberts, David and Richard Hayes. *Power to the Edge*. C4ISR Cooperative Research Program (CCRP), Washington, D.C. 2003, p. 27.

⁴² The United Kingdom further specifies the differences between network centric warfare and network enabled capability at the following site: <http://www.iwar.org.uk/rma/resources/uk-mod/nec.htm> 20 October 2004.

By exploiting technical connectivity and shared situational awareness, NEO can utilize processes for operations other than war. In these types of operations, unity of command is rare. However, because of the shared awareness and knowledge, individuals or groups can not only execute commands more precisely, but also make their own decisions more capably. Figure 3-3 shows how the NCW self-synchronized command and control process is multiplied and further decentralized when put into a network enabled environment in operations other than war.

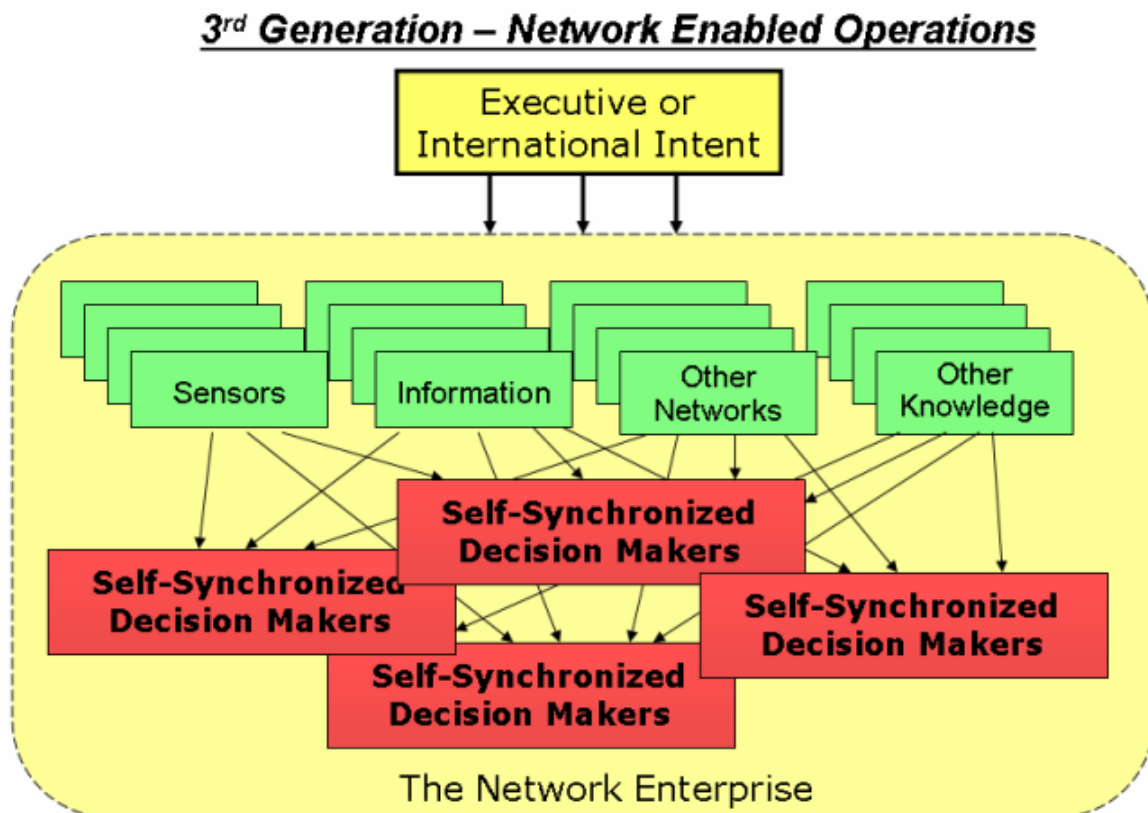


Figure 3-3. Expansionist View of Network Enabled Operations with Self-Synchronization Processes Embedded in the Overall Operations

An example of a situation that can exploit NEO is a conflict where multiple operations must be accomplished as quickly as possible. As an alternative to using the networked information simply to deconflict events geographically or sequentially, users share information to enhance each team's ability to accomplish its mission. For example, imagine a natural disaster, such as a major earthquake, occurring in the capital city of a

country with an already unstable government. Agile networks must quickly form to enable coordination of the international disaster relief teams, including rescue operation from multiple countries, food and shelter services provided by NGOs, and aid from the United Nations. Insurgents unhappy with the current government, however, take this opportunity to join forces with a terrorist organization from a neighboring country. They try to create havoc for the current government by thwarting international relief efforts. A coalition force is then tasked with counterinsurgency operations.

It is up to the military to form adaptable information and intelligence networks and provide the correct access to each member of multiple participating organizations. There is not necessarily unity of command since the operation is not strictly military; however, there is unity of effort as everyone understands their role in the relief efforts. Since speed saves lives in this case, it is important to allow a decentralized approach to command and control to exponentially increase the amount of decisions and actions that can occur simultaneously. The information sharing network is the key to providing synergy in operations. At the same time, these networks must be secure from the insurgents and terrorists. This scenario is similar to the fictional example in the draft version of the “Net-Centric Joint Functional Concept” due for signature in early-2005.⁴³

H. Issues with Networks

Before fully embracing either NCW or NEO methods, several challenges must be faced over the next several years. The first and most urgent problem is interoperability. Currently many DoD network systems do not work together. Competing protocols cause huge problems among the services. The major U.S. Army program for their digitized battlefield, called Force XXI Battle Command Brigade and Below (FBCB2), uses a message protocol and frequency spectrum that does not work with the active duty Air Force. The Air Force favors the Navy Link-16; however, their implementation differs

⁴³ The Draft Department of Defense Net-Centric Joint Functional Concept (Version 0.5), 1 October 2004, is expected for release early in 2005. One of the main topics of discussion in the working groups is still about the correct definitions and terms to describe these events. For this reason, I have chosen to continue using the term “NEO” even if this document uses the term “net-centric” (an adjective?) to describe the same thing.

causing system degradation when the Air Force and Navy operate on the same network. Meanwhile the Air National Guard chose a system that is compatible with the Army but requires a translator to talk with their active duty brethren. The Marine ground units bought the same data link radios as the Army, but has such a different concept of operations that the radios become doctrinally incompatible due to differences in network designs. Army Patriot sites use Air Force-Navy Link-16, but Army aviation did not procure Link-16 terminals. Additionally, due to integration problems and delays, the active duty F-16s just recently received their first data link radios and had to use a modem device to share information only with other F-16s during the Operation Iraqi Freedom. Finally, the newest aircraft, the F/A-22, does not currently share its data with the rest of the Air Force. This lack of interoperability is what military leaders call “stovepipes” because they transmit information only along single lines of communication instead of sharing data across other systems. In essence, this is similar to the Beta – VHS competition in the late 1970s or the MAC-PC competition of the 1990s. Either a single protocol needs to be established that wins the “marketplace” (the VHS solution) or a shared protocol that everyone can easily integrate (the Java Solution for Apple and IBM) must be developed. Otherwise, operators will never be able to adequately share knowledge. The Joint Tactical Radio System (JTRS) promises to do this, but is still many years from fielding.

One of the reasons that so many non-compatible systems exist is due to failures in the DoD acquisition process. While a new strategic triad has been established for the U.S. strategic posture, the old acquisition triad remains unchanged: 1) behind schedule, 2) over budget, and 3) does not meet expectations. Requirements have to be established years in advance of hardware integration into the system. The cycle time to update software in an aircraft is, at best, approximately 3-5 years. The acquisition process cannot keep up with the pace of technology. When trying to coordinate systems among several platforms, the timeline just gets longer. In fact, the cost to integrate systems across multiple platforms is enormous. NCW can only work if the money is budgeted for developing robust systems, promoting new concepts of operations, and cultivating well-trained operators. At the same time, it is critical to keep funding current systems. If too

much funding is allocated towards technology that does not yet exist, then current capabilities will suffer. Funding must be properly apportioned to meet current requirements and future growth. Capt Terry Pierce, U.S. Navy, author of *Warfighting and Disruptive Technologies: Disguising Innovation*, suggests a 90/10 split for current systems and investing in disruptive technologies.⁴⁴ No matter what the correct funding distribution is, the DoD needs an agile acquisition strategy to be flexible and responsive. Otherwise, the military is in for slow progress towards mature network enterprises.

Assuming compatible systems are integrated, information security becomes the utmost challenge. As operations become more reliant on shared information, security becomes an increasingly difficult issue. If an adversary taps into the network, all information is potentially compromised. An option would be to compartmentalize the information, but that goes against the concept of information sharing in the first place. Since these systems are to be used not just by the United States, but all coalition forces, it is much harder to track potential security leaks. Critical operationally secure information about troop positions and movements, weapons, force size, etc, could easily be compromised without U.S. knowledge.

Even without any security breach from adversaries, much of the information is classified. This requires not only a clearance, but also a need to know. If the data is just posted to the network similar to an internet web page, then there is no requirement for the user to establish a need to know before he has access to that information. Additionally, some critical information has always been close-held by certain organizations. NCW assumes that it is more important to share that information than to hide it from other organizations. This is counter to security paradigms and will require a major change in how organizations operate before NCW can realize its full potential.

Another challenge is the need for joint experimentation and training. These are critical to develop the new concepts associated with NEO and the information RMA. However, it is extremely expensive and time consuming to integrate all the necessary

⁴⁴ Interview with CAPT Terry Pierce, USN, October 2004. His book is: *Warfighting And Disruptive Technologies : Disguising Innovation*. London ; New York: Frank Cass, 2004.

assets for proper training. This greatly reduces the amount of practice possible. For many pilots, their only experience with a CAOC is at Red Flag exercises or when they arrive in theater. Unfortunately, squadrons go to Red Flag exercises less than once a year. Even then, only a portion of the squadron attends. Training at home will have severe limitations when other entities must be simulated. Integrating multiple assets into a consolidated training schedule will be required. It is critical to have a knowledgeable, well-trained force to conduct network centric operations. The military will need to provide the budget for recurring, robust, integrated experimentation and training.

Finally, what happens when the systems fail in the fog and friction of war? It is important to remember the nature of war still provides uncertainty even with the additional shared knowledge. A by-product of networked operations is the interdependency created among entities. However, no organization should be so dependent on outside entities that it would be impossible to accomplish their primary objective on their own. As an alternative, the focus should be on creating symbiotic relationships where entities help each other instead of depending on each other. As with any new capability, it is crucial to maintain tried and true autonomous tactics for contingency operations.

I. Can Self-Synchronization Be Achieved?

With these necessary conditions met for self-synchronization, this decentralized control structure has been demonstrated successfully. During Operation Iraqi Freedom, the mission of the western war team was to search and destroy weapons of mass destruction before the enemy could launch them. This was potentially the ultimate time sensitive target as any western SCUD launch could greatly affect the nature of the war. The players were identified early to include Joint and Coalition Special Forces; U.S. Air Force and Air National Guard fighter and gunship pilots; a handpicked CAOC team; intelligence, surveillance, and reconnaissance gatherers; and specialized communications experts to manage the data link infrastructure. Before the war, the team gathered in the United States to develop the operations concept, tactics, techniques, procedures, and network architecture. They trained together allowing time to develop trust in the

operators, CAOC team, network, and equipment. When the war began, almost all entities were equipped with data link devices and could share their position information with each other. Clear rules of engagement had been established which allowed the pilot to decide if he was clear to drop ordnance or if he required more information. For example, if he felt he could not make an adequate collateral damage estimate, he could call for support to get better sensor information at that position. If timing was critical (a SCUD launch in progress), he was clear to engage with no further coordination. The cockpit display showed the position of the ground friendly forces and emerging targets, greatly enhancing the pilot's SA and target acquisition confidence. All four self-synchronization conditions were met. Self-synchronization occurred allowing the pilots to work directly with Special Forces teams or on their own, servicing all intended targets. While no WMD were discovered, the mission was still a success. All possible target locations were surveyed, no SCUDs were launched, secondary targets were destroyed, and no fratricide incidents occurred from data-linked aircraft.

J. Summary

Network enabled operations expands network centric warfare and self-synchronization into the 21st century as the way the military will conduct operations. Just as the CommTech model demonstrates, effective linking among all entities will lead to decentralized decision-making and calls for a less controlling leadership style that promotes trust and influence.

NEO and self-synchronization are possible to achieve when the necessary conditions are met. Competent forces must have the opportunity to train together and build trust in one another. Trust must also exist not only between peers, superiors, and subordinates, but also in hardware and software reliability. High quality information provides shared situational awareness and enables network centric warfare to be successful. Finally, having a clear, consistent understanding of the commander's intent makes self-synchronization possible. With adapted command and control methods, appropriate doctrine, and proper organization, the military can exploit new technology to

better meet its objectives. The effects will be increased tempo, responsiveness, and combat effectiveness, thereby, increasing the overall efficiency of the military.

CHAPTER 4. BUILDING OPERATIONAL TRUST

A. *Introduction*

As the CommTech Model shifts towards a period of decentralized decision-making, new information technology affects the way the military conducts operations and fights war. Because web-design networking ensures everyone has better access to information, people will be more inclined to make their own decisions. Therefore, the likelihood that subordinates will blindly trust a commander and execute orders disappears as individuals accept the responsibilities that accompany decision-making. Alfred Lord Tennyson's famous quote from his poem, "The Charge of The Light Brigade," which says, "Their's not to reason why, Their's but to do and die,"⁴⁵ is no longer the military mindset in the latest decade of the CommTech model. Instead, individuals need a reason to trust.

The new generation of soldier, sailor, airman, and marine wants to know and understand why their squadron leader made the decisions he made. As teams become smaller and more dispersed, it is even more critical to trust the directions that come from geographically separated commanders if the teams are expected to follow orders. However, people build trust through experience and face-to-face contact with each other. Fighter pilots build trust with other fighter pilots by discussing the afternoon's training sortie over a beer together in the squadron bar. With geographically dispersed, networked forces, there is no opportunity for this.

To add to the problem, both network centric warfare and the future generation network enabled operations rely on interdependency for their success. This interdependence *requires* a level of trust to be successful. The authors of the book,

⁴⁵ Lord Tennyson, Alfred, "The Charge of the Light Brigade," *Poems of Alfred Tennyson*, J. E. Tilton and Company, Boston, 1866. <http://eserver.org/poetry/light-brigade.html>. 29 November 2004. The rest of this stanza is: "*Forward, the Light Brigade!*" *Was there a man dismay'd? Not tho' the soldier knew Someone had blunder'd: Their's not to make reply, Their's not to reason why, Their's but to do and die: Into the valley of Death Rode the six hundred.*

Power To The Edge, specifically state a necessary condition for self-synchronization is “Trust in the information, subordinates, superiors, peers, and equipment”⁴⁶ Can this condition be met?

Meeting this condition asks a lot from military leaders, decision-makers, operators, effectors, managers, industry – basically, everyone who is in some way involved with networking operations. Everyone knows that teams that work together can be more efficient, and a key aspect to working as a team is trusting one another. But trust is not something that can be ordered. You cannot expect people to trust each other just because someone directs them or it is part of the doctrine. Yet many people that discuss trust just expect it to be readily available regardless of its earned value. Instead, trust needs to be examined from a realist’s perspective. By examining the nature of trust, we can determine the factors it relies on. Perhaps, by concentrating on improving those factors in a network centric environment, we may be able to increase the level of trust among entities. This, in turn, will allow for more effective and efficient operations in network centric applications such as those involving self-synchronization.

This chapter tackles the requirement for trust in network centric warfare, self-synchronization, and network enabled operations. After explaining the concept of *Trust*, the chapter introduces a new concept called *Operational Trust*. It explains why there is a need for trust and offers factors that facilitate trust. Finally, it gives a real-world example of how the decision-making process involving trust demonstrates our need to develop systems, practices, and concepts of operations keeping in mind the need to trust.

B. A Definition of Trust

Since there is no single agreed upon definition of trust, I offer the following definition, which is tailored to the needs of operational missions:

***Trust is a bet that an entity, which you cannot control,
will meet expectations that are favorable to your cause.***

⁴⁶ Alberts and Hayes. *Power to the Edge*. C4ISR Cooperative Research Program (CCRP), Washington, D.C. 2003., p. 27.

Breaking down this definition, “trust is a bet” means that the person who must give trust – called the “trustor” – makes a speculation on whether his prediction will pay off. The trustor is always a person. Trust is a human behavior. Alice can trust that Bob will drive her safely to school. Bob can trust that his car will not breakdown. But the car cannot trust that Alice or Bob will not spill their drinks on the seats. The car is not capable of trust.⁴⁷

The aspect of the “bet” comes from Piotr Stompka’s treatment of social trust.⁴⁸ When you trust someone, you are placing a bet as to how he will act. If that person or entity acts correctly (in your perception) then you have won your bet. Trust paid off.

An “entity” refers to the object in which you place your trust—the “trustee.” This can be another person. It can also be an object such as a computer, radio, vehicle, any hardware, etc. Information can also be the object of trust. “I trust the information to be relevant, accurate, and timely” is a valid (perhaps far-fetched) statement. The trustee can also be a system or concept such as network centric warfare, democracy, America, or God. Receivers of trust are not required to be human.

“...which you cannot control...” is critical in defining trust. With total control over the trustee, there is no requirement to trust him. A sure bet is not really a bet; it is a guarantee. Trust happens when the outcome cannot be completely controlled. If there are areas where uncertainty can be reduced, then the bet will be easier to make. Hence, it becomes easier to trust. However, eliminating the uncertainty completely means there is no longer a requirement for trust.

The next section of the definition is “...will meet expectations...” Trust is a bet on the future. Based on a current assessment, you predict the future outcome of events. “Based on my assessment that I always receive mail on weekdays and today is a weekday, I predict that the mailman will deliver my mail today.” I do not have control over the mailman, but I have come to expect mail delivery, which makes it easy to predict

⁴⁷ Alice and Bob are the fictional characters that often appear in much of the *Trust* literature.

⁴⁸ Sztompka, Piotr. *Trust: A Sociological Theory*. United Kingdom: Cambridge University Press, 1999.

that he will stop by today. By allowing business associates to send correspondence to me, I am now placing trust in the postal service that they will deliver the mail. In other words, I place a bet that the mailman will deliver. It is an easy bet to make since he reliably delivers the mail every weekday, thus making the prediction fairly simple. If my prediction of the future turns out to be false, then I wrongly placed trust in the mailman, lost my bet, and will not receive that promised check in the mail.

This brings us to the final part of the definition: "...that are favorable to your cause." Just because you can predict an outcome does not make it the future you want. Trust is necessary for people to work towards a common goal. Results must be favorable. Otherwise, the expectation of occurrence is not trust. It is just something to recognize and tackle. For example, Alice can expect that if Bob drives her to school at 8:00 A.M., there will be traffic. Alice does not trust in the traffic, she predicts that it will be there and leaves a few minutes earlier to compensate for it. As another example, my sister has never arrived to anything on time in her entire life. If I trusted her to be on time to dinner, I would most likely be disappointed and eat cold food. But, I don't say that I put trust in my sister to let me down. I just predict it (and can even bet on it!). For this reason, trust requires predictions that will help the trustor's cause, not hinder it.

C. Moving from Blind to Reasoned Trust

Within this definition, there are two types of trust – blind trust and reasoned trust. Blind trust is the equivalent of making an uninformed bet. The blind trustor has no reason to believe the trustee will act honorably; however, she places her trust in that person or entity without hesitation. Reasoned trust, on the other hand, is the equivalent of making a smart bet. Having a reason to trust makes it easier to make the correct trust-based decisions. For example, if Alice goes to the racetrack and bets on a horse simply because it wears a purple jersey, that would be a dumb bet. However, if Alice does her research and finds that the horse with the purple jersey has won every race that year and is the offspring of Seattle Slew, then she has a good reason to bet on that horse. By having a reason to trust, not just having blind trust, people can make smarter decisions.

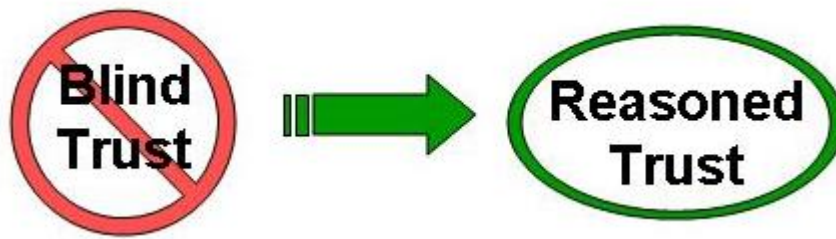


Figure 4-1. Moving from Blind Trust to Reasoned Trust

At times individuals may not have any reason to trust, yet they still do. Everyone has some baseline level of inherent trust in others, and some people are more trusting than others. For example, the other day, a lady standing on the corner of a busy intersection stepped off the curb into the crosswalk as soon as the light turned green, without a glance to see if the cross traffic had actually stopped. She had completely trusted that all other traffic would obey the laws of the road. What she missed by not glancing up was the taxi driver attempting to make the yellow light and then screeching to a halt just inches away from her. She would be considered a person with a very high baseline level of blind trust (or maybe she was just distracted by talking on her cell phone).

Observations obtained while living, working, and deploying with marines, fighter pilots, and special forces soldiers, suggest that this group, in general, has a very low baseline for blind trust. Fighter pilots tend to trust only other fighter pilots. Special Forces soldiers trust their team members. The marine motto, “Semper Fi” (always loyal) aims to provide a culture of trustworthiness, but does not create a trusting attitude towards non-marines. In other words, all others must earn these warriors’ trust before they will make decisions based on trust. Therefore, it is important to facilitate a means to gain reasoned trust in military operations.

D. Operational Trust

Having described Trust, I now offer a new concept – *Operational Trust*. Operational trust is the trust that is required from every person and earned by every entity

to accomplish an endeavor. Complex operations involve several entities, and this requires a certain level of interdependence. Each relationship requires a level of trust in order to complete the entire mission. By sharing knowledge and dividing workload, we become more efficient at accomplishing the mission. However, the more we interlink and share knowledge to accomplish a task, the more dependent we become on entities we do not necessarily control. As operations become more complex, no single person or even small team can accomplish all tasks required of a mission. At this point, trust is not only desired, but required to complete the mission.

Operational trust comes from a variety of perspectives. Warfighters must trust their peers, commanders must trust subordinates, and subordinates must trust their commanders. Operators must trust the equipment, and all players must trust in the tactics, techniques, and procedures. Moreover, the leaders of the overall operation must trust in the players to accomplish the endeavor in an ethical manner. In other words, a person has no choice but to give a level of trust to certain entities (people, objects, systems) in order to complete his mission.

An example of operational trust can be illustrated using the objective of the transportation system. Alice must drive in order to get to work. For her to be willing to get in the car, she must trust in the infrastructure – that the roads are well-paved; the traffic lights are correctly timed; the lines are painted on the ground. She must also trust in the equipment – her car is reliable; the tires hold air; the brakes can stop the car. She must trust the other drivers on the road – they will obey traffic laws; they will stay on their side of the road; they will avoid hitting her. She must trust in the doctrine and training system – everyone driving has learned the same set of rules as she.

If she does not extend trust to these entities over which she has no control, then she can choose not to drive. However, if she needs to drive to get to work to pay the mortgage to have a place to live, then she has to drive and she has to trust.

Her task in the overall mission is to drive to work and support herself. The Dept of Transportation's task is to build the roads and establish the policy so individuals can collectively support the economy. Congress appropriates funding for the national

highway system to support commerce which supports the economy. The Dept of Motor Vehicles' task is to ensure drivers are properly trained so they can safely drive to work and collectively support the economy. The task of the highway patrol is to ensure everyone is following the rules so that everyone can drive to work safely and support the economy. And so forth.

Every entity has a piece of the overarching operation. By accomplishing each individual portion of the mission, they collectively accomplish the overall endeavor. As entities interact during their individual tasks, however, they are affected by each other's actions. Therefore, they are required to extend a certain level of trust in order to carry out the mission. Alice could not drive to work (her role in supporting the economy) if she was not willing to trust the other drivers, roads, vehicles, law enforcement, etc.

The complexity of large operations brings about both a benefit and a byproduct. The benefit is the symbiotic relationship that forms among the different entities. All subgroups bring a contribution that helps the others in achieving their objectives. At the same time, a byproduct is formed – interdependence. We become dependent on the other entities to complete our mission.

The key difference in operational trust compared to other types is that this level of trust is required, not just desired. Otherwise, the mission success is either not achievable or, at best, completely inefficient. This is trust from a realist perspective. We cannot expect that by simply advocating that everyone trust each other, that operations will become more efficient. The reason to extend trust is because it is required to accomplish the goals in an efficient manner. However, by discovering ways to make trust assessments more precise, we can make decision-making easier and more correct. This will, in turn, make it possible to increase the efficiency and effectiveness of the overall operations.

E. How Operational Trust Factors In – Why It is Important to Network Centric Warfare

Because NCW gains its leverage from the concept of interdependency to provide shared knowledge, operational trust is critical to the success of the NCW missions,

especially self-synchronization. Linking information from multiple sources adds another degree of complexity to an already complex mission. The more entities that are involved with sharing information and dividing tasks, the more the requirement for trust grows. Operational trust is the lynchpin in all networked operations.

Due to the uncertainties of near-future threats, we need to be prepared to fight any enemy, anywhere, at any level of conflict, from enforcing sanctions and capturing terrorists, to full-scale theater operations and nuclear war. We require agile, adaptable command and control networks to respond to any given situation. This will require the synergy inherent in networked operations to provide the accuracy, relevance, and timeliness of the target information under an increased operations tempo.

Unfortunately, many understand a need for trust, but do not address how to develop it. Sweeping statements like “Everybody should just trust each other more and we will all work together better” conjure images of flower children dancing in green fields. However, trust is not something that you can expect everyone to just give freely. Trust must be earned, and correct decision-making depends on the individual’s ability to assess and appropriately place trust. The rest of this chapter focuses on determining the requirement to trust and how to make it easier to extend trust.

F. Understanding the Need to Trust

When determining the need to trust, two main questions come to the mind of the trustor: 1) Do I have to trust? and 2) What are the risks involved? To help explain these questions, I have created an example scenario that uses a network centric application thread, Time Sensitive Targeting (TST) with Blue Force Situational Awareness (Blue Force SA). In this scenario, the Blue Force fighter aircraft must eliminate a mobile surface-to-air missile (SAM) site as quickly as possible to maintain air superiority. This will, in turn, allow the flight to continue with close air support (CAS) missions supporting dispersed Army special teams on the ground.

In this example, we take the perspective of “Thud,” the lead F-16 fighter pilot of a flight of four aircraft carrying high-speed anti-radiation missiles (HARMS) and precision guided munitions. However, to fully understand operational trust, the same process must

be applied from the perspective of the Army teams, the air-C2 node, the ground forward air controller (FAC), the combined air operations center (CAOC), the regional combatant commander, and any other player involved in the mission.

Step 1. Determining the Need to Trust: *Do I have to make a bet?*

Three factors play a role in determining the need to trust:

a) **Importance of my task** – This first step is to determine how critical my own task is in the overall success of the operation. How much are others depending on me to complete my task successfully? How trustworthy do I need to be so that others can trust me? This is where having a clear understanding of the commander's intent is so crucial. Every player must understand what the commander's intent is to be able to assess the importance of his task in the overall mission and to understand how other tasks depend on his success. In our scenario, Thud and his wingman need to destroy the mobile SAM site so that the other element of his flight will be able to provide CAS without being shot down. The Army teams are depending on the F-16's weapons for support against enemy fire. The other aircraft in the area, such as JSTARS, AWACS, and tankers, need Thud to destroy the SAM so they can continue their missions controlling the fighters. Failure to complete the mission successfully could have consequences across the spectrum from personal (getting shot down) to tactical (losing aircraft) to operational (inability to provide CAS to Army troops) to strategic (the Army unable to achieve their objective on the ground due to lack of air support) to political (CNN films the Coalition army absorbing huge casualties). Thud's mission is, therefore, very important and he is required to be trustworthy.

b) **Necessity of dependency** – Do I need help to accomplish my tasking? Whom and what do I depend on to complete my mission? Thud cannot find this SAM site on his own without risking being shot down. He needs the support of sensor platforms such as JSTARS and satellites to pinpoint the location of the threat. He needs the target analysts to provide an accurate assessment of the location and lethality of the threat. Their assessment is critical to his attack on the target. There must also be a reliable process in

place to convey the target information to the pilot. Furthermore, Thud needs his wingman to protect him from immediate enemy fire while finding and destroying the target.

c) **Amount of dependency** – How critical is each of these dependencies? Do I have alternatives? Before the advent of radios, commanders had to convey detailed rigid plans in advance, hope their men fully understood the orders, and trust they would carry them out. Mid-course corrections required messengers running to the front line – if they made it. There were few alternatives. Changes in technology and tactics enable contingencies and alternate methods more readily. This means there can be less dependency on certain entities with redundant capabilities. In this case, the choice of options may be prioritized to achieve efficiency or convenience.

Returning to the scenario, Thud depends on the network data link to provide the information into his cockpit for rapid targeting. If the data link fails, however, he has an alternate, but slower, way to receive the information (e.g. voice communications). Therefore, depending on the urgency of the situation, the data link may or may not be critical for his success. Is the data link a convenience that makes him operate more efficiently, or will it increase the safety of the mission? How often has he practiced the alternate methods? As the alternative approaches become less practiced, his dependency on the data link network increases. This will factor in to the amount of trust he is required to give the data-linked information in the future.

Step 2. Assessing the Risk: *What are the stakes of the bet?*

At this point, Thud has decided whether he needs to extend trust. Now comes the question of assessing the risk. It is important to recognize the potential negative consequences of misplaced trust in the wrong entity. Depending on the severity of the consequences, this will affect the decision to place trust in certain entities or continue to look for other options. The amount of risk can be determined using a risk assessment matrix, illustrated in Figure 4-2:

Risk Matrix	Probability of Occurrence				
Severity of Negative Consequences		Highly Unlikely	Not Likely	Likely	Highly Likely
	Minor	Green	Green	Green	Yellow
	Major	Green	Yellow	Yellow	Red
	Catastrophic	Yellow	Red	Red	Red

Figure 4-2. Risk Assessment Matrix for the Potential Consequences of Misplaced Trust

a) **Severity of Negative Consequences** – This step addresses the severity of the consequences if the entity in which you placed your trust defects. In other words, if the trustee fails to meet my needs, how will that inhibit my ability to accomplish the mission successfully? Thud is trusting that the data link will display the correct SAM information in his cockpit for quick efficient targeting. If the information does not come through, then he must get on the radio and go through the lengthy process of passing coordinates and target information by voice. This will delay his attack on the SAM. The delay may also allow time for the SAM to fire at the Blue Force aircraft. Or the delay could cause him to be too low on fuel by the time he gets the information confirmed that he is no longer able to service the target. If there are multiple SAM targets in the area, the slower communications mean he may be able to engage only one target during his sortie.

A potentially more dangerous scenario is that the data link information that arrives in his cockpit is wrong. If he does not recognize the “defection of the trustee” – the data link providing inaccurate information – then Thud may continue on the wrong target run-in, and fly directly over friendly troops. Wrong information is often more lethal than missing information because it might not be recognized that the information is wrong.

However, missing information that goes unrecognized, for example, Blue Force friendly positions not appearing, can also be lethal. What if the data-linked information displayed the location of the target, but not the location of the friendly Special Forces team that was also on the ground destroying it at the same time. Thud and his wingman

could easily deploy their weapons without knowing that friendlies were in the area. Depending on how coordinated the targeting data was when the analysts were consolidating the information, they may be unaware of the additional Special Forces team that is already in place destroying the SAM. If Thud unquestioningly trusted the data link target information provided by the analysts in the CAOC without receiving the Blue Force SA, he runs the risk of causing a fratricide incident. The higher the risk, the higher the stakes are to trust.

b) **Probability of occurrence** – Addressing the second part of the risk matrix, I must determine the likelihood that my trustee will fail in his part of supporting your mission. What is the probability that the entity in which I place my trust defects? This can be based on several factors. How difficult is the trustee's task? How much experience does the trustee have in accomplishing this task? How trustworthy is the trustee? How much does the trustee need to depend on others to complete his tasking? How many steps along the way need to take place correctly for the end to be successful? What are his other requirements that may conflict with your needs? These issues need to be properly assessed to understand the stakes, or likelihood, of the trust bet ending in your favor.

Returning to our scenario, Thud needs to trust his wingman. Properly assessing his wingman's capabilities, attitude, and primary mission will help Thud determine the likelihood of his wingman living up to Thud's expectations or not (in other words, will he cooperate or defect). In this scenario, Thud's wingman is carrying the high-speed anti-radiation missiles (HARMs) needed to suppress the SAM, which will enable Thud to get in close enough to the threat to be able to destroy it with his precision guided bomb. We have already determined this is a necessary role for the overall accomplishment of the mission. Since Thud is not carrying his own HARMs, he must rely on his wingman to accomplish his tasking before Thud can safely complete his. Luckily, Thud has been training with his wingman for several months and knows he is a competent pilot and trusted friend (which came from drinking beers together in the squadron bar).

If his wingman were new to the mission, he may not be able to achieve his objectives under the stress of enemy fire. In other words, the probability of negative

consequences increases even if the wingman intended to achieve his portion of the mission, but still does not complete his task. Thud is able to make an adequate judgment on his wingman's capabilities because he knows him personally, has trained with him in the past, and has prior knowledge of his wingman's capabilities.

Turning Thud's trust towards another recipient, we look at the controller who passes the targeting information through the data link network to Thud. The controller's tasking is complex in that it depends on several correct correlation processes happening in the CAOC for the target information to reach him correctly. He must correctly interpret the data and match up the best aircraft suited for the mission (in this case, Thud's flight) in addition to assessing the situation in the airspace. Thud has never met the controller directing his attack, but he estimates that most of them are young airmen with little experience. Thud does not know this individual's level of training but has to trust that the training system has brought him up to an adequate level. Can Thud make a good assessment about the trustworthiness of his controller? In addition, Thud is expected to trust the data link itself. If the information just appears on his screen without some sort of verbal confirmation from the controller, then Thud does not know if the information is really intended for him or if it is just a glitch in the system. Since the network design is an extremely complex process, the data link could easily send accidental data flowing to the wrong place until all the bugs are worked out. The probability of any new network breaking your trust is generally high. Without prior knowledge and experience with the people on the other end of the computer network, Thud will generally be conservative in his risk assessment. Therefore, Thud will most likely assess the risk as high until he has collected some past experience with the controller and the specific network design. Thud's ability to develop a good assessment of the probability of defection occurring is necessary to adequately evaluate the risk of trusting.

G. Finding Ways To Make It Easier To Trust

Now that we know that it is necessary to trust certain entities, and we have assessed the associated risk, we can start to look for ways to mitigate the risk. This starts

by making a better prediction of the trustee's actions. By knowing what to expect, it is easier to identify if and when an entity is defecting. The trustor also has more of an opportunity to reduce the severity of negative consequences by identifying alternatives sooner, correcting the situation, or beginning damage control. By reducing the risk, it makes trust easier to accept. Facilitating trust will lead to better operational decision-making, which will, in turn, lead to more efficient and effective operations.

Step 3. Changing the Odds: *Can I make a safer bet?*

The next seven areas contribute to making a better bet by reducing the uncertainty. In other words, these areas will help the trustor move from blind trust to reasoned trust. This will make it easier to make that trust bet, which correlates to faster, more efficient decision-making:

a) **Situational Awareness (SA)** – SA is a trust enabler because it greatly enhances the operators ability to make predictions about trust. Situational awareness is “the knowledge, cognition, and anticipation of events, factors and variables affecting the safe, expedient and effective conduct of the mission.”⁴⁹ It is developed through the continuous integration of new observations into recurring mental assessments. This is the stage of the OODA loop where the decision-maker orients himself to everything going on around him. The analogy of trust and SA is if trust represents the future, then SA is the equivalent for the present. Situational awareness provides the current reasoning to make the trust bet.

By having a good mental picture, I can better predict the next set of events around me. For example, as I am driving my car, I like to know what vehicles are around me and their relative speeds. By knowing the placement of the other cars, if an unexpected dog jumps in front of my car, I know which direction I can swerve while still avoiding crashing. This also requires knowing the maneuverability of my car and the conditions of the road to avoid skidding. If I am driving in an unfamiliar rental car and it is snowing, I

⁴⁹ This definition comes from Taylor, R. M. (1990). “Situation awareness rating technique (SART): the development of a tool for aircrew systems design.” *Situational Awareness in Aerospace Operations* (Chapter 3). France: Neuillysur-Seine, NATO-AGARD-CP-478. <http://www.raes-hfg.com/crm/reports/sa-defns.pdf> 19 May 2004.

may have more attention focused on just driving and be less aware of the traffic around me. Being less prepared for the unexpected puts me in a more dangerous position due to lack of SA.

Good SA will greatly increase Thud's ability to predict future actions or recognize when events are not working out as planned. This is where the data link has proven to be truly invaluable. By having near real-time information of the friendly ground and aircraft positions, Thud is much more able to accomplish his mission without a fratricide incident. Sharing this information among his fellow pilots gives them a common picture. Therefore, he can be more certain about his wingman's level of SA also.

However, bad data can cause a decrease in SA. For example, data-linked position information is actually where the object (aircraft, vehicle, person) *was* when the radio transmitted it. Depending on how fast they are moving or the update rate, the data could be anywhere from several seconds to several minutes stale. There also may be no indication to the pilot how stale the data points are. During the final run-in stage of attacking a target, it is critical to have not "near real-time," but actual real-time information on the friendly positions in the area. This is especially true for CAS missions where ground troops are always in close proximity to the targets.

Our pilot, Thud, uses his SA to predict how events will unfold and to recognize quickly when they are not as expected. For example, if he sees that his wingman is flying out of position, he may be alerted that his wingman's SA has dropped (perhaps due to an avionics restart in his aircraft) and needs some time to rebuild his mental picture. Thud's SA can also help him predict the accuracy of the AWACS surveillance information, such as a neutral aircraft, as it appears on his display. If he believes there are errors in the position being reported, he could point his radar in the direction of the neutral aircraft and refine the data coming to him through the data link. When he receives bad data into his cockpit, such as a hostile aircraft at his location, if his SA is high, he can determine that there is an error in the information and he is being incorrectly displayed to others as the enemy. This adds to his experience base when evaluating how much trust the AWACS crew deserves from him.

Situational awareness is key to developing good predictions, which are required to be able to trust other entities. The better my SA, the easier it is to extend trust because I will be able to quickly recognize if events are transpiring as predicted or not. By maintaining a more complete understanding of the surrounding situation and circumstances, I will be better able to predict follow-on actions, even those you cannot control. This will allow trust to be extended more easily.

b) **Verification (both during and after)** – Part of building a good mental picture is being able to distinguish good information from bad. Having an ability to verify the information is a simple way to accomplish this. Tools that allow someone to crosscheck information will help them quickly ascertain the accuracy and sometimes even the relevance of the information. This verification process can also help correlate multiple pieces of information in order to decrease the error in all of them. For example, a global positioning system (GPS) receiver works in this manner to determine its precise location.

One of the major benefits of network centric warfare is its ability to link information to gain a shared awareness of the battlespace. In 20th century warfare, verification of information was accomplished through a hierarchical chain of command. This approval process provided the checks and balances required to feel confident in committing to action. With self-synchronization, the players at the edge need to have their own system of verification in order to know the information they are receiving is valid. Thud is an example of an edge player who needs to be able to confidently assess new information to build and maintain his SA, and consequently be able to trust the other players he depends on.

In network centric warfare, multiple sensor types in different parts of the electromagnetic spectrum can be used to verify the location and targeting information of the SAM. By collecting and crosschecking this information with each sensor, the analyst that fuses all of the observations can feel very confident predicting the target's exact location. If all that information is consolidated in the CAOC and only the final answer is sent to the fighter, however, then the fighter has limited capability to verify the target information in his own cockpit. This may reduce his trust or at least cause him to believe

the stakes are higher in granting trust. His SA has effectively been reduced by not having the ability to see some of the information that led to concluding the target was valid.

In this case, Thud may have to just accept the higher risk in trust – call it blind trust – where he has no choice but to trust and no way to reduce the risk. However, if he is able to use his own onboard sensors, such as his radar or targeting pod, to correlate the coordinates, then he can verify the target appears to be in line with other information. A key difference between simple network centric operations and self-synchronization is that, with the latter, the effectors – the guys actually dropping the bombs – must have the ability to assess the trustworthiness of the data. It cannot be left up to the CAOC or other C2 platforms to just issue a “Trust Me” card. Everybody is responsible and accountable for self-synchronization to work.

c) **Past Experience** – Another way to improve the prediction is to have past experience with the trustee. The more I get to know how someone responds to different situations, the more likely I will be able to predict how he will respond in future interaction. The same logic goes with equipment. The more familiarized I am with a system, the more I understand its capabilities and limitations. When these systems become critical to the mission, I will already have experience with them and know how well they work. While this seems obvious, it underscores the need to train together. By practicing the mission with the same team of people, the same equipment, and the same procedures, everyone will be better prepared to trust each other and accomplish the real mission just as they have trained.

The U.S. Joint Forces have put new emphasis on effects-based operations. Yet training still focuses on small pieces of the mission. Aircraft squadrons train together to practice their specific tactics required to target a SAM, but rarely train with the operators and controllers that they will undoubtedly be linked with during real operations. Large joint and combined exercises are difficult to plan and coordinate, and expensive to budget. If forces do not train jointly, then how can they develop the past experience together to build trust in each other’s capabilities? Since one of the key concepts to network centric warfare is that entities can be geographically dispersed, maybe it is possible to plan for more training opportunities across elements of a mission without the

cost of training deployments. In addition, if bases took the initiative to plan low-level training exercises with nearby posts, relationships could form allowing each unit to find the other more trustworthy. As these relationships form into packaged mission sets, then it would be beneficial to deploy the joint package together to meet real operational requirements.

d) **Indirect Reputation** – Another option if personal experience is not possible is having indirect knowledge of the reputation of the entity. The Army ground FAC may not know Thud personally, but he may have had several occasions working with Thud's squadron. If he develops an opinion that the people in the squadron are competent and trustworthy, then he can extend this level of trust to the squadron members he has yet to work with. By sharing experience bases of a group with individuals, the Army FAC can make a prediction of the competency of Thud's flight. The indirect reputation to show trustworthiness can also come from Thud working with another trusted member of the Army team who vouches for Thud. While indirect reputation does not provide as good a prediction as direct experience, it can still make it easier to extend trust.

e) **Amount of Control** – How much control do I have over the actions of other entities? As flight lead, Thud has a measurable level of control over his wingmen, since he directs their actions in the mission. Pre-established power and command relationships come into play, but that may not be enough. Based on the training and experience together, Thud can assess how much control he has over the flight. For example, if a new, inexperienced pilot is flying, he may be more likely to act unpredictably due to lack of training. This equates to having worse odds in the trust bet. The more control Thud has over the situation, the less risk he has to take. This equates to making it easier to trust. He may be more willing to make that bet.

How easy is it to control people through a data link without face-to-face contact? That depends on how well the trustor knows them or how much he has worked with them. It might also depend on how closely they follow the planned tactics, technique, and procedures. Again, it is based on past experience that will determine a fair assessment of control over the situation.

Furthermore, the amount of control an operator has over a given piece of equipment is directly related to the human factors design of the system. For example, some radios, such as a survival radio may be designed to be foolproof and have very few switches that can be adjusted. But in doing so, it limits the capabilities of the radio and leaves the survivor with less control. On the other hand, the combat search and rescue team has better control over the survivor because they know he cannot change the frequency or try to do something with the survival radio that it was not designed to do.

f) **Finding a Common Cause or Objective** – Another way to reduce the uncertainty in a trustee's actions is to assess whether there is a common objective. If both the trustor and the trustee are working toward the same cause, then they will be more motivated to be trustworthy. While each achieves his objectives, each one also helps the other achieve his, creating a win-win situation.

With NCW and especially self-synchronization, one of the necessary conditions for successful operations is having clear command intent. This will ensure that people understand their role in the overall mission. It will also help ensure that both you and your trustee realize that you are both working for the same mission. This will allow both of you to extend trust more easily. In other words, the best way every player can feel easier about extending trust is for everyone to clearly understand the overall mission and their role in it. This is best accomplished by having a clear commander's intent.

g) **Likelihood of Future Interactions** – Finally, the last factor to make it easier to trust is the likelihood of future interactions with the same trustee. Future interactions are sometimes needed to keep people trustworthy. If they expect or fear reciprocal treatment, then they will be more likely to do what is expected of them. If there is no chance of future interaction, then the trustee has no fear of reprisal, and he is free to act in a less favorable manner. For example, if Bob stops at his hometown cafe for breakfast, receives good services, and then does not tip the waitress, there is a possibility that she will remember him next time and provide bad service. In this case, the waitress placed trust that Bob would follow custom if he received good service. The likelihood of a future interaction between Bob and the waitress ensures that Bob will meet her prediction. On the other hand, if Bob stopped at a truck-stop diner that he never intends

to visit again, he could easily save his money by not tipping and get away with it. However, just because there is no future interaction does not mean that Bob cannot be trustworthy; it only means that future relationships can act as a warranty for Bob to live up to the trust bestowed upon him.

By flying together Thud and his wingman have a common mission even with different roles. The next time they fly, their roles may be switched. Either way they will mutually support each other as they have learned to do on every mission they fly together.

H. A Real-World Example of Trust in the Decision Process

To tie the factors regarding operational trust to network centric operations and self-synchronization, this chapter closes with a real world example that demonstrates the aspects discussed above. In some ways it worked well, in others it did not. While it shows how trust affects the decision process, it also shows how far we need to come to co-evolve technology, tactics, conops, and training with operational trust in mind.

During Operation Iraqi Freedom (OIF), I witnessed a close-call in a potential fratricide incident. The problem began when a computer restarted at a location geographically separated from the point where the incident was unfolding, but still linked through the network. When the computer restarted, it opened its transmit filters, and at the same time, began transmitting stale targeting data over data link network. The location that the data pointed to was of a target that had been destroyed days earlier, and a Special Forces team was already working in that vicinity. However, the stale data passed machine-to-machine through an air control squadron, which automatically transmitted the false data over the air. At this point, the target information then took on the reputation of the air control squadron transmitting it. What the fighter aircraft received in his cockpit was target information of a hostile target coming from an authoritative control element.

What saved this from becoming a terrible situation was the pilot making a proper assessment of trust while, at the same time, flying his mission over enemy territory. Because of the nature of the operation, he knew the importance of his mission and the need for the data link to provide timely, accurate, relevant information to him. He also

recognized the potential consequences of acting on incorrect information over the link. Luckily, this was an experienced pilot with very high SA at the time. He had also witnessed, in the past, glitches with the network. While the data link was putting out false targeting information, it also had Blue Force friendly positions in the vicinity being displayed correctly. Because the pilot's SA was high, he was able to notice that the two sets of overlaying data did not correlate. It did not make sense to have friendlies and hostiles at the same location. Since the data link in his aircraft was a relatively new system and the network in OIF was extremely complex, he did not place a high level of trust in the system. Through voice communications, he was able to verify which piece of information was correct. He was also able to inspect the target with on-board sensors to further verify that the operators had also made a correct assessment of the ambiguous information being displayed. In this case, the fratricide was avoided.

However, due to the urgent nature of destroying time sensitive targets, a pilot with less SA might have engaged the target based on the direction from the data link. If this occurred, what would the mishap investigation discover? Who would be held accountable for the lethal error? Would the pilot who dropped the bomb feel guilt-free because he was following the direction of the computer? Would the air control squadron be held accountable since the target information had their computer stamp on it? What about the designers of the computers that attach to the network? The bottom line is that accountability of information on a network must be traceable and verifiable not only during post-event investigations, but also real-time. Where and when the data truly originates is a critical factor in deciding the level of trust in the data. People mentally assess the timeliness, accuracy, and relevance based on who is transmitting it. Any operator on the net deserves to know the source.

I. Summary

While this last example demonstrates a failure in the networked system, it also demonstrates the successful decision making process associated with assessing trust. This example is here to show everyone how far we have come in network centric warfare, but at the same time, how much farther we need to go to get it right. Operational trust is

the lynchpin in all networked operations. By taking into account the process people go through to develop and extend trust, perhaps we will be able plan for these factors. This will be even more critical as we move closer to decentralized network enabled operations.

Networked systems need to be designed with the components of trust in mind. But it is not just about the design of the data link systems. Networking operations require the co-evolution of doctrine, concepts of operations, force structure, and tactics. These, too, must incorporate the human element of trust in decision-making during development, operations, and training.

Network centric warfare, self-synchronization, and network enabled operations, are, no doubt, the direction the latest technology will take us. But we must develop it smartly with operational trust in mind. Facilitating trust will support better operational decision-making, which will lead to more efficient and effective operations.

CHAPTER 5. NETWORK LEADERSHIP STRATEGY AND TACTICS

A. *Introduction*

This chapter pulls together all previous chapter lessons as it addresses the question, “What can our leaders, and even we as leaders, do to capitalize on the Information Age?” The simple answer is threefold: provide good influence, improve network conditions, and build operational trust.

At a recent workshop discussing the future of network centric warfare, the following statements were made at the outbrief:

Leadership development must be focused on developing leaders who have knowledge and skills that are relevant to the information age and competent to the times. Leadership will need to deal with the dispersion of authority and responsibility across the set of temporary and informal organizational structures that will evolve under collaboration.⁵⁰

Leaders must learn the skills to influence their subordinates, peers, and even their commanders, if they want to hold power in the new network environment. This chapter delves into ideas that address these challenges to leadership. It provides specific ways to shape network culture and “operationalize” trust in networks for effective operations.

B. *Leadership Strategy*

First, control is out – influence is the key to successful leadership in the new network organizations. Leaders need to communicate a clear, consistent message to subordinates to ensure they direct their efforts in a manner that aligns with the overall strategy. Furthermore, they must believe in and pass on to others the same message that their own leaders are espousing. Therefore, it is critical to have clear executive vision and command intent for any operation. Included in this must be the operational priorities,

⁵⁰ Net Centric Joint Functional Concept Workshop Outbrief. July 2004., <http://www.netcentricfcb.org/NCFCBWorkshop3.html> 18 November 2004

functional doctrine, operational perspectives, proper guidance, ethical standards, appropriate rules of engagement, and well-defined roles and accountabilities.

Leaders must create the vector. With the rise of networking information, innovative capabilities will rise from the bottom-up, providing the magnitude. Leaders must provide the direction – the vision – to drive the organization forward. Gareth Morgan writes, “Transformational leaders need to transmit their vision into reality, their mission into action, their philosophy into practice....Alterations in communication, decision-making, and problem-solving systems are tools through which transitions are shared so that the visions become a reality.”⁵¹

The leader and the entire organization must commit to the vision daily. By setting the standard for the organization, he will provide the expected framework for his subordinates to follow. Lower-level troops want to understand the significance of their orders. They need to know how their work fits into achieving the mission. Effects based operations consider how daily tasks align with the bigger operational goal. If a Stryker brigade is to attack a target, the brigade members should know how that target fits in with the overall objectives of the mission. In a decentralized environment, it is important to provide, not only the goal, but also the ethical manner and approach to reach that end-state.

Generals and Admirals must shift into the “mentor” mindset. Dr. Thomas Malone, founder and director of the Massachusetts Institute of Technology Center for Coordination Science, suggests a new kind of C2 – instead of command and control, at the strategic level, shift to coordinate and cultivate.⁵² The new generation of soldiers, will not just follow orders, they will make decisions. Unfortunately, even if they are not competent, they may still think they are; plus they will have the power and ability to make bad decisions. Every soldier, sailor, and airman should be given a course in critical

⁵¹ Morgan, Gareth, *Creative Organization Theory*, p.165.

⁵² Malone, Thomas, *The Future Of Work: How The New Order Of Business Will Shape Your Organization, Your Management Style, And Your Life*. pp. 129-131.

thinking and ethical decision-making.⁵³ It is essential that they have the skills to make good decisions. Since people's perspectives change as they gain experiences in life, this course should be repeated every few years in an effort to "re-cage" good decision-making characteristics.

This leads into the next point: Know when *not* to trust. This thesis is not about learning to trust each other – it is about making good decisions based on an accurate assessment of trustworthiness. Along that vein, we can make more decisions to act in parallel if we can create an environment of trust. This will produce faster, more efficient operations, which is, of course, the end goal. However, blindly placing trust in an incompetent person causes negative ripple effects to everyone who depends on the success of that element of the mission. If the risk assessment matrix presented in Chapter 4 (Figure 4-2) indicates high risk, it is important to remember to analyze other options.

It is also important to check your own situational awareness (SA). Some commanders believe they always know the right answer. Streaming video in the CAOC only serves to reinforce that belief. However, the insidious problem with SA is that people do not recognize when they have lost it until they regain it. Also, they are unaware of the pieces of information that are missing. Once a commander makes his decision, he has a strong tendency to stick with that solution, regardless of further evidence to suggest a better solution. The tendency to disregard negative information, called a confirmation bias, has led commanders and their troops on to horrific blunders. Commanders must be willing to hear dissension and negative information to keep their SA in check. Furthermore, although a commander sitting in the operations center may have access to hundreds of information sources, he still does not have the complete picture of the ensuing battle on the frontline. Dr. Milan Vego, professor of Joint Military Operations at the Naval War College, concludes: "It is an illusion to think that senior

⁵³ Professor George Lober's class on Critical Thinking and Ethical Decision-Making (NS4710) at NPS is an excellent example of the coursework and discussions that should be proliferated to the entire Department of Defense.

leaders can grasp tactical intricacies better than their subordinates. Nor can they take advantage of their fleeting opportunities on the ground.”⁵⁴

We expect decentralized decision-making to be effective, but we have not given the edge organizations the tools yet to perform this task. Leaders must make an effort to get the frontline warfighter what he needs, instead of bringing all the new technology to the CAOC. To make *informed* decisions, warfighters need to have reliable conduits for information flow. Many systems have been developed that provide specialized needs to small units. However, they were created without considering how they will interoperate with other systems. These systems carry the brand “stovepipe” to portray their characteristic single source, single direction information flow. Many military leaders would like to crush these programs, but have a difficult time because the individual system is so well liked by the community that uses it. Instead, leaders should encourage development of simple translators and connectors to provide information cross-flow. The stovepipes are not the problem; it is the lack of venting between them that causes havoc. By cross-flowing data across multiple systems, operators have a greater possibility of receiving the information and thus making better decisions. This also applies to more tacit information. Leaders should encourage cross-flow of tactics, techniques, and procedures across joint boundaries. As more ideas are shared, new improvements will arise. This innovation should be encouraged.

Finally, turn those “Iron Majors” into “Golden Majors.” In a speech given at the Naval Industry Conference earlier this year, Admiral Ed Giambastiani, Commander USJFCOM, remarked: “Examples of [transformation concepts] ..., I am happy to report, are being deployed right now in the combatant commands – our primary JFCOM customers. But I will tell you that the process is painful and slow. We have found that there is great agreement on the process-and-products of joint transformation at the most senior level and down among the troops who have fought as a joint force. They ‘get it.’ But the ‘iron middle managers’ – the majors, lieutenant colonels and colonels that we have trained to protect service programs, authorities and resources – pose a significant

⁵⁴ Vego, Milan N. “Operational Command and Control in the Information Age,” Joint Forces Quarterly. Issue 35. 2004. pp.100-107.

challenge.”⁵⁵ Instead of allowing iron majors to thwart innovation, leaders should get them onboard with the idea early in the process. Then they will be the vehicle to sell new transformational concepts to the troops.

C. Influence Techniques – Specific Tools for Soft Power

Throughout this thesis, I have stressed the need to develop skills to exert softer power by focusing on influence instead of direct control. However, so far there have yet to be any specific methods, only generalities. The next several paragraphs will discuss some specific techniques to persuade superiors, peers, and subordinates to follow your vision and direction. These techniques are discussed in detail in the book, *Influence: The Psychology of Persuasion*, by Dr. Robert Cialdini.⁵⁶ Although this book is mainly directed at the consumer and marketing audience, the same techniques can also apply to situations where military leaders must persuade others. However, while many of the examples in the book show the abusive power of influence, these techniques are offered in hopes they are used for good, not evil.

1. Provide a Reason

According to Cialdini, people are more willing to do what you ask if they know the reason. This matches with the CommTech Model prediction that as subordinates gain access to other sources of information, they will be less likely to blindly follow orders. They want to know why. But we may underestimate the power of this method of persuasion. In some cases, even playing the trump card, “Because I said so,” may be a valid enough reason if used only sporadically. In 1978, Dr. Ellen Langer conducted an experiment measuring the power of the word “because.” The results are clear in the following excerpt:

Langer demonstrated this unsurprising fact by asking a small favor or people waiting in line to use a library copy machine: "Excuse me, I have five pages. May I use the Xerox machine because I'm in a rush?" The

⁵⁵ Giambastiani, Ed, Commander USJFCOM, in remarks for the Naval Industry Conference, 4 August 2004, <http://www.jfcom.mil/newslink/storyarchive/2004/sp080404.htm>. 1 September 2004.

⁵⁶ Cialdini, Robert B., *Influence: The Psychology of Persuasion*. New York: William Morrow, 1993.

effectiveness of this request plus reasons was nearly total: 94 percent of those asked let her skip ahead of them in line. Compare this success rate to the results when she made the request only: "Excuse me, I have five pages. May I use the Xerox machine?" Under those circumstances, only 60 percent of those asked complied. At first glance, it appears that the crucial difference between the two requests was the additional information provided by the words because I'm in a rush. However, a third type of request tried by Langer showed that this was not the case. It seems that it was not the whole series of words, but the first one, "because," that made the difference. Instead of including a real reason for compliance, Langer's third type of request used the word because and then, adding nothing new, merely restate the obvious: "Excuse me, I have five pages. May I use the Xerox machine because I have to make some copies?" The result was that once again nearly all (93 percent) agreed, even though no real reason, no new information was added to justify their compliance."⁵⁷

2. Gain Commitment

By simply gaining commitment from others, they will likely remain loyal to the cause and follow through with the mission. An early lesson in basic training is the importance of integrity. Once a soldier gives his word, he will consider it a lapse of character to change his mind. According to Janus and Mann, prominent social psychologists, once people make a difficult decision, they become more confident in that decision.⁵⁸ This phenomenon, called bolstering, has been documented even in horseracing, where bettors feel more confident in their horse after they make their bet.

One way to gain that commitment is to start small and build. For example, the Chinese communists used this foot-in-the-door approach of indoctrination in the prisoner of war camps during the Korean War.⁵⁹ While this example is negative in context, it shows the power of this approach to persuasion. Starting with asking prisoners to agree with simple, harmless statements like, "The United States is not perfect," led to further admissions where prisoners gave specific examples of U.S. imperfections. Eventually, they found themselves entering essay contests glorifying communism. By actually

⁵⁷ Cialdini, Influence: *The Psychology of Persuasion*, p. 4.

⁵⁸ Lebow, Richard. *Between Peace and War: The Nature of International Crisis*. The Johns Hopkins University Press. Baltimore, Maryland, 1981. pp.104-107.

⁵⁹ Cialdini, pp. 69-80

writing the essay, not just saying it, the concepts became further engrained into the prisoners' minds, until they truly internalized the benefits of communism. Repeated short-term compliance can often lead to long-term cultural shifts. Moreover, the prisoners' written statements could be shown to others, thus convincing fellow prisoners it was acceptable to enter the essay contest.

Convincing several people to commit to a cause has a two-fold benefit. First, people are much more willing to go along with something if they see others doing it too. Just as a crowd of people looking at the sky causes a passerby to look up also, a team member is likely to concur if he sees the rest of the team conforming. The second benefit is the domino effect leading to a "tipping point."⁶⁰ By convincing people to internalize an idea, they become the new spokesmen, spreading the idea at an exponential rate. Once a concept is adopted by enough people, it reaches a tipping point where acceptance by the masses is inevitable. Consider how the idea of "targeting specific people" was completely unacceptable as a form of warfare before the war on terror began. By 2004, both presidential candidates were liberally using the phrase "hunt them down and kill them" in campaign speeches to cheering crowds. This example shows the snowball effect that can occur when an idea hits its tipping point.

3. Start Early

Try to introduce your idea before other ideas are on the table. Garner consensus in the early planning stage. That way the others become the alternatives, which require significant scrutiny before the first idea can be ruled out. The best psychological operation is one that makes the first impression. The reason this is such an effective tactic is due to what Robert Jervis calls "cognitive consistency." Jervis states, "The principle of consistency helps us to make sense of new information as it draws upon our accumulated experience, formulated as a set of expectations and beliefs. It also provides continuity to our behavior."⁶¹ We look for confirming evidence and tend to disregard

⁶⁰ Gladwell, Malcom, *The Tipping Point: How Little Things Can Make A Big Difference*, Boston: Back Bay Books, 2002. This book explains in detail the process and requirements to reach a tipping point.

⁶¹ Lebow sites Robert Jervis from *Perception and Misperception in International Politics*. Princeton University Press. Princeton, New Jersey, 1976. pp 17-42.

disconfirming evidence. The earlier an acceptable idea is embedded into our brains, the more likely we are to find further justification that it is correct.

However, beware of your own irrational cognitive consistency in decision-making. Jervis continues, “The pursuit of consistency becomes irrational when it closes our minds to new information or different points of view....Persistent denial of new information diminishes our ability to learn from the environment.” Someone who becomes over confident in his beliefs may tend to disregard experiences causing misperceptions and irrational decision-making. In other words, be willing to accept others’ ideas if they are better than yours.

4. Benefit from Reciprocity

Take care of your troops and they will take care of you. By giving to others, not only will they appreciate it, but they will also feel indebted to you. Consider the marketing campaigns where free address labels are sent to your house along with a letter asking for a donation. Even though the labels were unsolicited, many people feel that they must reciprocate for the gift even if they never use the labels. Nice deeds build a sense of obligation and loyalty. Favors beget other favors; this is exactly how political parties build alliances to gain a majority vote. While most people do not like to admit being a part of political games, they should realize it is an irrepressible outcome of network organizations. Therefore, you may as well accept it and be good at it. Furthermore, reciprocity can have an escalating effect. After all, how much do you donate for fifty cents worth of address labels?

5. Appearance Builds Respect

Regardless of whether or not it is fair to assess someone’s capabilities based on personal appearance, several studies have proven people are more willing to listen to someone who is attractive. According to Cialdini, “we automatically assign to good-looking individuals such favorable traits as talent, kindness, honesty, and intelligence.”

Furthermore, we do this without being conscious of it.⁶² Personal appearance can reflect much more than just good genes. It is an expression of your health, fitness, attention to detail, and ability to take care of business. In the military, even more so, troops will be more inclined to trust and respect a commander who is athletic and in good shape, even if his job involves only sitting behind a desk. If you are fat and out of shape, the thought process of others is, “How can you take care of the mission and the troops if you can’t even take care of yourself?” In 2004, the Chief of Staff of the Air Force General John Jumper introduced a new program, “Fit to Fight,” which specifically aims at creating a healthier, more respected, force.

Besides appearance, mannerisms can also be an effective influencing tactic. Solid eye contact, good posture, and a firm handshake give an immediate first impression of an ethical, honest, upfront person. Excitement in a project can be infectious to others. By sounding authoritative, people will believe you are an authority. On the other hand, stuttering or sounding unsure will make people question your ability to command troops or manage a project. You will have a difficult time convincing even subordinates to listen to you if you cannot command their respect.

6. Build a Cohesive Team

In network enabled operations, team members will come from multiple organizations and form quickly to meet the given challenge. Any team will work better if they are a cohesive force. One method to influence this is to get “buy-in” from all team members on the mission, tasks, roles, contracts, expectations, and end-state. Find similarities or common interests; having common experiences can help instill trust. Create a symbol that is specific to the team. Shared symbols are a simple way to build pride and cultural unity in a newly formed team. As the team performs well, that symbol becomes recognized as part of the reputation of the team. Consider how emblems such as a Special Forces badge or a Weapons School graduate patch instills pride in all members, or how others reverently call test pilots “golden arms” when they see the patch on their flightsuit sleeve.

⁶² Cialdini, p. 171.

7. Choose the Technique to Fit in Context

Every situation and every person is different. There is no all-encompassing technique that will always work. It is important to use the right influence technique for the right situation. Do your research beforehand; strategize a plan to sell your plan. Know your target audience and use an approach that will produce the desired behavior. Whether the right approach is a carrot or a stick, a good leader will know which method will be the most effective on each specific target. If you need buy-in from a specific individual who has reservations, get the person to explain what the specific issues are. That way you can address each concern and win support.

D. Some Final Thoughts For Implementation

Listed below are a few ideas that could bring about more efficient operations in future network enterprises. These concepts have not been thoroughly vetted through the DOTMLPF process. They are listed here as a spring board for future thoughts. By paying attention to the trust and influence lessons described in this thesis, military organizations can become more efficient network operators.

1. Create Capability Thread Teams

When U.S. forces go to war, they fight jointly, but they rarely train that way. There are limited opportunities to train as we fight. However, planning staffs expect that a “plug-n-play” force will be prepared to operate together with effective results. The actuality is an ad hoc group with no established reason to trust, a misunderstanding of cultural barricades, and inefficient operating conditions. Furthermore, these problems provide justification for theater commanders to centrally control the mission events. Instead, we should create small joint teams that perform a complete end-to-end capability thread. These teams will train *and* deploy together.

Colonel Lou Durkac, USAF Air Combat Command, recently applied this concept by proposing what he called a Joint Mission Capability Package for Synchronized Air-Ground Operations at the Coalition Ground Forces Light Armored Vehicles

Conference.⁶³ He addressed the problem that light armor vehicles (e.g. Strykers) require air power to engage heavy enemy forces and provide air defense. Airpower needs agile ground forces to dislodge heavy enemy forces and act as forward air controllers. By creating small teams of Strykers plus F-16C+s (which already have interoperable data link and communications systems) that train together and deploy together, this force package will be ready to fight efficiently on Day One.

2. Create Competition Exercises

With mission oriented teams, training could involve an annual event where these teams compete against each other for “Top Gun” accolades. The benefits are three-fold. 1) Competition will inspire teams to train harder and work better together. 2) Competitive “Type-A” warfighters will create innovative new tactics to win events. Since the proof is in the award, these innovations can be quickly shared across the communities. And 3) Winners gain a recognized reputation as “the best of the best.” When called into a combat theater, that reputation will deploy with them.

USSTRATCOM has continued the tradition from its predecessor, Strategic Air Command, of annual Guardian Challenge or Olympic Arena Events. At this tournament, each base sends their best missile launch and maintenance crews to compete for first place honors and base reputation recognition. This concept needs to be shared outside of the strategic nuclear forces community.

3. Create Reputation Scores

When direct experience is not possible, indirect reputation can help provide adequate reason to trust. What if every military member maintained a reputation score, similar to a credit score or an eBay score? Perhaps they could be split to include capability, dependability, and security trustworthiness. Inputs would come, not just from experience and formal processes, but also from closed-loop feedback of peers, superiors, and subordinates. When new agile teams are forming, the team leader could use these

⁶³ Durkac, Louis M. “Stryker / F-16C+ Joint Mission Capability Package for Synchronized Air-Ground Operations.” Presented at the IDGA Light Armored Vehicles Conference, Washington, D.C. 1 December 2004.

reputation scores to build his perfect team. Furthermore, just as committed eBay sellers follow through on every sale, individuals would work harder to ensure their score remained unblemished.

4. Cultivate a Dedicated Infrastructure Force

The person responsible for all communications links in a theater of operations is called the Joint Interface Control Officer (JICO). Currently there are only a handful of qualified JICOs across all branches of service, and after gaining specific knowledge, they often return to their previous career fields. The job entails having a solid understanding of both the technical design and operational uses of several different communications networks. Because of the intricacy and speed of new technology, by the time they become truly capable JICOs, they move on to their next assignment.

In the Combined Air Operations Center, decisions depend on the network infrastructure, yet little thought or praise is given to the JICO cell when everything is operating correctly. (At the current state of technology, it is a miracle that the systems stay on line and function together as well as they do.) JICO teams are augmented with several civilian contractor experts to hold the web together.

However, if the network communications are such an important part of command and control, why do we not have our own organic capability to manage the infrastructure? We need to cultivate a JICO force as a specialty-coded career field and take care to manage their careers. For example, the exceptional JICO, who created and held together the largest data-linked network to date for Operation Iraqi Freedom, was recently passed over for promotion. As one of a select few with the most operational experience in network infrastructure, he has since been sent back to his old career field.

5. Simplify the Process for Innovation

More and more people have great ideas, but what is the military process for turning the great ideas into real combat capability? Small communities have put procedures in place to share requirements and solutions within the community. For example, Air Combat Command holds its annual weapons and tactics conference to

discuss requirements and upcoming capabilities. However, when an idea crosses joint boundaries, the method becomes lengthy, convoluted, and difficult to figure out. Furthermore, enlisted soldiers and officers alike do not know how to begin the process. The result is that the top flag officers will decide the warfighter requirements and solutions instead of the men and women on the forward edge. This is counter to the concept of letting capabilities bubble up.

Another similar example comes from recent first-hand experience. While conducting research for this thesis, I was sent an electronic copy for review of a draft concept document about the transformation to network operations along with directions for submitting comments. All comments required staffing through a general officer or equivalent for submission. It seemed ironic that the coordination process for a document about network transformation required a hierarchical approval procedure, thus countering what the document espoused in the first place. If we expect to encourage innovation, we need a well-defined simple process that everyone knows how to do. Perhaps we need to reinvigorate the Suggestion Form 1000 program for joint force applications.⁶⁴

6. Visit the Squadron Bar

This statement is not meant to glorify alcohol. It is meant to give due reverence to the camaraderie and trust that develop on Friday afternoons. But it is more than mere friendship that forms. Some of the greatest ideas have come from collaboration after work hours, recorded on cocktail napkins. In Tucson, Arizona, Air National Guard pilots, frustrated with the amount of time it took to coordinate a laser guided bomb attack, concocted a new capability that took advantage of their new tactical data link equipment. Over a few beers, they designed a new technique to share all relevant targeting information and laser codes across the data link, resulting in cooperative precision attacks with increased confidence, reduced time, and minimal voice communications. The

⁶⁴ The Suggestion Form 1000 was a popular process in the late-1980s and 1990s where anyone could submit any cost-saving idea, from removing expensive missile caps before test launches to installing motion detector light switches in building to reduce electricity costs. If the program was adopted, the submitter received a check for 10% of the first-year cost savings.

cocktail napkin design sped quickly through the requirements vetting process in time for the next software upgrade. The Cooperative Lasing Mode (a.k.a. “CLAM” Mode) was in the jet within the year.

E. Summary

The military must be prepared to transform its organization, doctrine, strategy, and tactics to co-evolve with technology. Only then will we truly benefit from the changing capabilities created by the Information RMA. By understanding what the changes are and how they affect us, we will be better prepared for the future global environment. All warfighters should consider how to best exploit information to increase our combat capability.

CONCLUSION

Christopher Evans, a computer scientist and avid science fiction enthusiast of the 1970s, predicted in his book, *The Mighty Micro*, that the “computer revolution” would lead to globalization, the rise of the third world, the decline of communism, free and easy information exchange, and an end to war as we know it.⁶⁵ He was correct.

Communications technology has led to the information revolution in military affairs. This is reshaping how we plan, operate, educate, organize, train, and equip forces for the 21st century. The CommTech Model presented in this thesis shows how communication technologies affect our organization, leadership style, and decision-making process.

Networking enables every individual from the top battle commander to the lowest echelon fighter to share information and gain increased situational awareness. However, sharing information allows individuals to feel capable of making their own decisions with increased confidence. Rank within a hierarchical organization becomes less relevant as a source of power, as subordinates question orders or find ways around roadblocks in the chain of command.

Therefore, leaders must create the vector – the direction – to drive the organization forward. Commanders must communicate a clear, consistent message that includes (but is not limited to) command intent, guidance, objectives, operational priorities, rules of engagement, and ethics. Operational trust is the lynchpin for networked operations. Leaders must learn the skills to influence their subordinates, peers, and even their commanders, if they want to hold power in the Information Age.

Network Centric Warfare and Network Enabled Operations provide the framework for integrating information technology into the battlespace. While the debate regarding how best to operate in a networked environment continues, both camps clearly see the benefits of shared situational awareness. Consequently, it is crucial that we get the technology, and hence capability, to the warfighter in the field.

⁶⁵ Evans, Christopher, *The Mighty Micro*, Gollancz, London, 1979. Unfortunately, Mr. Evans died in 1979, before he had the opportunity to see his predictions materialize.

THIS PAGE INTENTIONALLY LEFT BLANK.

BIBLIOGRAPHY

- "Air Force Doctrine Document 1." (17 November 2003).
- "Net-Centric Joint Functional Concept (Version 0.5) *DRAFT*." (1 October 2004).
- "Apple-History.com" [cited 6 December 2004]. Available from <http://www.apple-history.com/frames/>.
- "Brainyquotes. com." [cited 1 December 2004]. Available from http://www.brainyquote.com/quotes/authors/r/rosalynn_carter.html.
- "The FY 1999 Defense Budget And Future Years Defense Program, Chapter 21 " [cited 6 December 2004]. Available from <http://www.defenselink.mil/execsec/adr98/chap21.html>.
- "Operation El Dorado Canyon." [cited 26 October 2004]. Available from http://www.globalsecurity.org/military/ops/el_dorado_canyon.htm.
- "President George H.W. Bush's Address Before A Joint Session Of The Congress On The State Of The Union. 28 January 1992." in Reprinted on C-SPAN.org [database online]. Available from http://www.c-span.org/executive/transcript.asp?cat=current_event&code=bush_admin&year=1992
- "The Sontay Raid." [cited 26 October 2004]. Available from <http://www.psywarrior.com/sontay.html>.
- Air Force Experimentation Office. "Joint Expeditionary Force Experiment (JEFX) 2004 Quicklook Results and Initial Recommendations." (September 2004).
- Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing And Leveraging Information Superiority*. Washington, DC: National Defense University Press, 1999.
- Alberts, David S., and Richard E. Hayes. *Power To The Edge: Command, Control In The Information Age*. Washington, DC: CCRP Publication Series, 2003.
- Arquilla, John, David F. Ronfeldt, United States. Dept. of Defense. Office of the Secretary of Defense, and National Defense Research Institute. *In Athena's Camp : Preparing For Conflict In The Information Age*. Santa Monica, Calif.: Rand, 1997.
- Arquilla, John, David F. Ronfeldt, United States. Dept. of Defense. Office of the Secretary of Defense, Rand Corporation, and National Defense Research Institute. *Swarming & The Future Of Conflict*. Santa Monica, CA: Rand, 2000.

- Arquilla, John, David F. Ronfeldt, United States. Dept. of Defense, and National Defense Research Institute. *The Advent Of Netwar*. Santa Monica, CA: Rand, 1996.
- Axelrod, Robert M. *The Evolution Of Cooperation*. New York: Basic Books, 1984.
- Builder, Carl H., Steven C. Bankes, Richard Nordin, United States. Dept. of Defense. Office of the Secretary of Defense, and National Defense Research Institute. *Command Concepts : A Theory Derived From The Practice Of Command And Control*. Santa Monica, Ca.: Rand, 1999.
- Carter, Louis, David J. Giber, and Marshall Goldsmith. *Best Practices In Organization Development And Change : Culture, Leadership, Retention, Performance, Coaching : Case Studies, Tools, Models, Research*. San Francisco; Lexington, MA: Jossey-Bass/Pfeiffer; Linkage, Inc., 2001.
- Cebrowski, Arthur K., and John J. Garstka. "Network-centric warfare: Its origin and future." *United States Naval Institute.Proceedings* 124, no. 1 (1998): 28.
- Cialdini, Robert B. *Influence : The Psychology Of Persuasion*. Rev. ed. New York: Morrow, 1993.
- Coram, Robert. *Boyd : The Fighter Pilot Who Changed The Art Of War*. 1st ed. Boston: Little, Brown, 2002.
- Directorate for Operational Plans and Joint Force Development, Joint Staff. "An Evolving Joint Perspective: U.S. Joint Warfare and Crisis Resolution In the 21st Century." JROC Memorandum 022-03.
- Durkac, Louis M. Colonel. "Stryker / F-16C+ Joint Mission Capability Package for Synchronized Air-Ground Operations " .
- Edwards, Sean J. A. *Swarming On The Battlefield : Past, Present, And Future*. Santa Monica, CA: Rand, 2000.
- Evans, Christopher Riche. *The Mighty Micro : The Impact Of The Computer Revolution*. London: Gollancz, 1979
- "Remarks for the Naval Industry Conference." Washington, D.C. [cited 1 September 2004]. Available from <http://www.jfcom.mil/newslink/storyarchive/2004/sp080404.htm>.
- Gladwell, Malcolm. *The Tipping Point : How Little Things Can Make A Big Difference*. 1st Back Bay pbk. ed. Boston: Back Bay Books, 2002.
- Hayes, Robert H. *Operations, Strategy, And Technology : Pursuing The Competitive Edge*. Hoboken, NJ: Wiley, 2005.

- Hehs, Eric. "USAF Weapons School, Training Weapon Officers at Nellis AFB, NV — April 1995." *Code One Magazine* (April 1995).
- Jasper, Scott E. "Transforming Joint Warfighting Capabilities." *Joint Force Quarterly : JFQ*, no. 35 (2004): 69.
- Jasper, Scott, and Michael Binney. "Joint Close Air Support Training Transformation." *Marine Corps Gazette* 88, no. 5 (2004): 71.
- Jasper, Scott, and Michael Binney. "Joint Close Air Support Training Transformation." *Marine Corps Gazette* 88, no. 5 (2004): 71.
- Jervis, Robert. *Perception And Misperception In International Politics*. Princeton, N.J.: Princeton University Press, 1976.
- Kidder, Rushworth M. *How Good People Make Tough Choices*. 1st ed. New York: Morrow, 1995.
- Kunz, Christine L. "OIF info 'brain'." *Airman* 47, no. 10 (2003): 22.
- Lebow, Richard Ned. *Between Peace And War : The Nature Of International Crisis*. Baltimore: Johns Hopkins University Press, 1981.
- Malone, Thomas W. *The Future Of Work : How The New Order Of Business Will Shape Your Organization, Your Management Style, And Your Life*. Boston, Mass.: Harvard Business School Press, 2004.
- Malone, Thomas W., Robert Laubacher, Michael S. Scott Morton, and Sloan School of Management. *Inventing The Organizations Of The 21st Century*. Cambridge, Mass: MIT Press, 2003.
- Morgan, Gareth. *Images of Organization*. 2nd ed. Thousand Oaks, Calif: Sage Publications, 1997.
- Morgan, Gareth. *Creative Organization Theory : A Resourcebook*. Newbury Park, Calif: Sage Publications, 1989.
- Nikolai, Douglas. "Centralized Execution of USAF Air and Space Forces: The Unspoken Trend of the Master Tenet (Classified and Unclassified Versions)." Ph.D. diss., September 2004.
- Pierce, Terry C. *Warfighting And Disruptive Technologies : Disguising Innovation*. London ; New York: Frank Cass, 2004.
- Rumsfeld, Donald H. "Transformational Planning Guidance." (April 2003).

- Szewczak, Edward, and Mehdi Khosrowpour. *The Human Side Of Information Technology Management*. Harrisburg, PA, USA: Idea Group Pub., 1996.
- Sztompka, Piotr. *Trust : A Sociological Theory*. Cambridge, UK ; New York, NY: Cambridge University Press, 1999.
- Taylor, R. M. *Situational Awareness in Aerospace Operations* France: Neuillysur-Seine: NATO-AGARD-CP-478, 1990.
- Tennyson, Alfred Tennyson, and Hammatt Billings. *The Poems Of Alfred Tennyson, Poet-Laureate Of England*. Boston: J. E. Tilton and Company, 1866.
- "Network Enabled Capability." [cited 20 October 2004]. Available from <http://www.iwar.org.uk/rma/resources/uk-mod/nec.htm>.
- Tichy, Noel M., and David O. Ulrich. "SMR Forum: The Leadership Challenge--A Call for the Transformational Leader." *Sloan Management Review (pre-1986)* 26, no. 1 (1984): 59.
- Vandenbroucke, Lucien S. *Perilous Options : Special Operations As An Instrument Of U.S. Foreign Policy*. New York: Oxford University Press, 1993.
- Vego, Milan N. "Operational Command and Control in the Information Age." *Joint Force Quarterly : JFQ*, no. 35 (2004): 100.
- Von Fremd, Mike. "Priority Mail: Determined Mom Helps Soldier Son Fighting in Iraq " *ABCNews.Com* (19 May 2004).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Major Nicole Blatt
US Joint Forces Command / J-9
Suffolk, Virginia
4. Mr. Shane Deichman
US Joint Forces Command / J-9
Suffolk, Virginia
5. Colonel Louis Durkac
ACC/DRG
Langley AFB, Virginia